



Board of Studies

**The Institute of Chartered
Accountants of India**

(Set up by an Act of Parliament)

ADVANCED INTEGRATED COURSE ON
**INFORMATION TECHNOLOGY
AND SOFT SKILLS (AICITSS)**

PART-A
ADVANCED INFORMATION TECHNOLOGY
MODULE 1

ADVANCED INTEGRATED COURSE ON INFORMATION TECHNOLOGY (AICITSS)

COURSE MATERIAL MODULE - I



Board of Studies

The Institute of Chartered Accountants of India, New Delhi

Advanced Integrated Course on Information Technology and Soft Skills (AICITSS) Part-A (Advanced Information Technology)

The objective of the Study Material is to provide teaching material to the students to enable them to obtain knowledge in the subject. In case students need any clarifications or have any suggestions for further improvement of the material contained herein, they may write to the Joint Director, Board of Studies.

All care has been taken to provide interpretations and discussions in a manner useful for the students. However, the Study Material has not been specifically discussed by the Council of the Institute or any of its Committees and the views expressed herein may not be taken to necessarily represent the views of the Council or any of its Committees.

Permission of the Institute is essential for reproduction of any portion of this material.

© THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior permission, in writing, from the publisher.

Basic draft of this publication was prepared by CA. (Dr.) Rashmi Goel

Updated Edition	:	January, 2025
Committee/Department	:	Board of Studies
E-mail	:	helpdeskadvitt@icai.in
Website	:	www.icai.org
Sale Price	:	₹ 720/- (For All Modules)
ISBN	:	978-93-48313-58-4
Published by	:	The Publication & CDS Directorate on behalf of The Institute of Chartered Accountants of India ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi – 110 002 (India)
Printed by	:	Sahitya Bhawan Publications, Hospital Road, Agra – 282 003 January 2025 P3760 (Updated)

PREFACE

Over the last two decades, Information Technology (IT) has made a significant impact on several accounting-related professions and practises. The organisations are significantly impacted by the cutting-edge developments in an array of IT tools and techniques.

To keep CA students abreast with the latest developments in the field of Information Technology, the Institute of Chartered Accountants of India has made earnest effort to revise its AICITSS – Advanced Information Technology (Advanced IT) curriculum to make it contemporary under its New Scheme of Education and Training. The uniform and synchronized imparting of the course is carried out by the Institute through its own IT Labs equipped with computers of latest configuration, software and other infrastructural facilities at almost all its branches and regional offices.

The topics covered through Advanced IT curriculum has been a stepping stone in building the IT skill set of the students. Taking the established knowledge base to the advanced level, the curriculum of Advanced IT has been revised that contains following major highlights:

- **Forensic Accounting and Fraud Detection** is an upcoming field that blends Auditing, Accounting, and Investigatory skills to assess financial documents. Forensic Accountants often review accounting systems and practices related to criminal and legal investigations.
- **Data Analytics Tools** such as MS Power BI, Python and KNIME are undoubtedly most user-friendly tools and are being extensively used all over the world. These tools would enable the students to work on cleaning and analyzing the big data, making quick reports, and providing actionable insights in terms of dynamic dashboards for informed decisions.
- **Digital Forensic and Cyber Security** is gaining lot of importance as all our assets and our lives are virtualized and have gradually moved to Cyber world and there is greater temptation to steal assets. Digital forensics is concerned with the identification, preservation, examination and analysis of digital evidence. Aspiring Chartered Accountants would have great scope in these areas.
- The curriculum is well equipped with the topics like **Advance Database Application using MS Access, Advance ERP Concept and Auditing of Financial Business processes using SAP / Oracle / MS Dynamics;** so as to make the budding professionals market ready and meet out the expectations of the competitive environment.

This course material has been prepared by Board of Studies of the ICAI in accordance with the course contents covered in the specially designed curriculum to disseminate quality education to its students.

We hope that this course material would help the students in building their IT skills which is a must for all, in the current scenario.



The Institute of Chartered Accountants of India

(Setup by an Act of Parliament)

Board of Studies

INDEX

Topic	Page No.
UNIT-1: FORENSIC ACCOUNTING AND FRAUD DETECTION	1
Chapter 1: Investigation	3
Chapter 2: Law Related to Fraud and Forensic Accounting and Investigation Standards	15
Chapter 3: Financial Transactions and Fraud Schemes	32
Chapter 4: Forensic Accounting–Data Sources from Different Websites	39
Chapter 5: Fraud Prevention and Deterrence	52
UNIT-2: BASICS OF DIGITAL FORENSIC AND CYBER SECURITY	57
Chapter 1: Introduction to Cybercrime	59
Chapter 2: Recent Trends in Cybercrime, Cyber Frauds in Financial Sectors	69
Chapter 3: Modus Operandi In Cyber Crimes	78
Chapter 4: Importance Of Digital Forensics & Ethical Hacking	92
Chapter 5: Digital Forensic Process	109
Chapter 6: Information Technology Crimes and Its Legal Consequences	120
Chapter 7: Digital Forensics Tools and Usage of OSINT Tools For Cyber Forensics	128
Chapter 8: Digital Forensics in Auditing & Forensic Accounting	160
UNIT-3: ROBOTIC PROCESS AUTOMATION	205
Chapter 1: Technology And Its Effective Use in Finance & Accounts	207
Chapter 2: Introduction To Robotic Process Automation (RPA)	209
Chapter 3: Impact Of RPA	215

Topic	Page No.
AUDITING OF FINANCIAL BUSINESS PROCESSES	
UNIT-4: ORACLE FUSION ERP	223
Chapter 1: P2P Cycle Audit	225
Chapter 2: Order to Cash Audit	250
Chapter 3: Fusion - Audit	280
UNIT-5: MICROSOFT (MS) DYNAMICS	287
Chapter 1: Explore The Core Capabilities of Microsoft Dynamics 365 Finance and Operations Apps	289
Chapter 2: Describe Reporting and Integration Capabilities in Finance and Operations Apps	307
Chapter 3: Learn The Fundamentals of Microsoft Dynamics 365 Finance	336
Chapter 4: Describe The General Ledger in Dynamics 365 Finance	357
Chapter 5: Describe Accounts Payable and Accounts Receivable in Dynamics 365 Finance	375
Chapter 6: Explore Expense Management, Fixed Asset Management, And Budgeting in Dynamics 365 Finance	394
TASK & KNOWLEDGE STATEMENTS	413



UNIT

1

Forensic Accounting
and Fraud Detection

CHAPTER 1

INVESTIGATION



LEARNING OBJECTIVES

- Forensic Accounting
- Investigation
- Theories used in Forensic Accounting
- Net Worth Theory
- Expenditure Theory
- Investigation Approaches
- Investigation Using Financial Data
- Investigation using Intelligence

1.1 FORENSIC ACCOUNTING

- Forensic Accounting refers to the examination of accounting records for potential financial crimes.
- More of investigative type, this would focus on going to grassroot levels to find out any sort of manipulation has taken place
- It has become relevant due to the growing number of frauds and failure of the so-called traditional mechanisms to detect and prevent the same.

1.2 INVESTIGATION

- A Main Characteristic that a Forensic Accountant should possess is the investigative approach.
- The Saying Goes “Auditor is a Watchdog not a bloodhound” and this is true in case of an auditor wherein the auditor should be like watchdogs having an eye on the financials like a watchdog and not be like the bloodhound type searching for errors.
- When it comes to a forensic accountant, rather the statement should be reversed -as the technique here would be like a bloodhound, being the breed that is used for hunting.
- Here forensic accountant would hunt for information in pursuit of his work and would be more like a hunter and more aggressive in approach.

1.3 PROCEDURE FOR FORENSIC AUDIT INVESTIGATION

Now let us learn the various investigative mechanisms in detail-here we focus on the case of Under reporting of income or suppression of income.

1.4 THEORIES USED IN INVESTIGATION IN FORENSIC ACCOUNTING

There are two theories commonly used in Forensic Accounting

- Net Worth Theory
- Expenditure Theory

Let's Discuss each of these theories in detail.

1.5 NET WORTH THEORY

- This theory focusses on tracing out the Unreported Income and is mostly used to find cases of Tax Evasions
- In this Method, the Net Worth of the Person as at the beginning and end of the Reporting Period, i.e. Financial Year is calculated
- The Change in Net worth is ascertained by subtracting the Opening Net Worth from the Closing Net Worth
- The Personal Expenditure incurred and Family spending during the year is then added to the Change in Net Worth and the resultant figure is taken as Gross Income
- There may be instances of Cash hoarded which has to be reduced from the Gross Income to arrive at the correct Gross Income
- The Gross Income Value is compared with the Reported Income which is the income declared as per Income Tax Returns

To understand this concept better lets take an example

The following table represents the Assets, Liabilities and personal expenses of Mr and Mrs Baburao from FY 2019-20 to FY 2021-22

No	Item Description	2019-20	2020-21	2021-22
1	Assets-Year ended	78,21,058.00	1,59,36,150.00	2,71,56,125.00
2	Liabilities- Year ended	21,11,147.00	47,22,164.00	68,15,280.00
3	Net Worth- Year ended	57,09,911.00	1,12,13,986.00	2,03,40,845.00
4	Increase in Net Worth (Opening as at 01.04.2019 is 31,15,911)	25,94,000.00	55,04,075.00	91,26,859.00
5	Personal Expenses and Family Spending	12,11,140.00	46,15,235.00	68,73,112.00
6	Gross Income (4+5)	38,05,140.00	1,01,19,310.00	1,59,99,971.00

According to this theory, the increase in Net Worth and the Personal Expenses should be covered by Income.

The difference between this constitutes the Income which is not reported by the Tax Payer

Lets now analyse the Gross Income and the Income reported by Mr and Mrs Baburao for the Years 2019-20, 2020-21 and 2021-22

No	Item Description	2019-20	2020-21	2021-22
1	Gross Income	38,05,140.00	1,01,19,310.00	1,59,99,971.00
2	Income as Reported	23,17,621.00	64,28,636.00	97,46,333.00
3	Additional Income	14,87,519.00	36,90,674.00	62,53,638.00

In the given case, there has not been adjustment made for the Cash Hoarded during previous years and in case there is cash hoarded the same would be reduced from Gross Income while proceeding ahead with the Calculation for Additional Income/ Non Reported Income,

Lets Presume there was cash hoarded to the tune of Rs.2,15,000 for the FY 2016-17, Rs,1,35,000 for FY 2017-18 and Rs,1,15,000 for FY 2018-19 Calculation will be revised as

No	Item Description	2019-20	2020-21	2021-22
1	Gross Income	38,05,140.00	1,01,19,310.00	1,59,99,971.00
2	Income as Reported	23,17,621.00	64,28,636.00	97,46,333.00
3	Cash Hoarded	4,65,000.00*	-	-
4	Additional Income	10,22,519.00	36,90,674.00	62,53,638.00

*Total Cash Hoarded from FY 2016-17 to FY 2018-19 is Rs.465000 (215000+135000+115000)

PROBLEM 1

Mr. Pillechan has reported the Incomes for the years as follows: -

Description	2019-20	2020-21	2021-22
Income as Reported	2,31,76,210.00	7,42,86,360.00	8,74,63,330.00

The Details regarding Assets and Liabilities are furnished below

No	Description	31.03.2019	31.03.2020	31.03.2021	31.03.2022
1	Assets	7,21,61,000.00	13,10,25,610.00	28,15,01,200.00	44,11,75,160.00
2	Liabilities	2,06,20,000.00	4,71,11,200.00	9,81,21,670.00	13,12,16,100.00

If the Personal Expenses and Family Spending for the Years 2019-20, 2020-21 and 2021-22 amounted to Rs.47,15,300, Rs.67,12,350 and Rs.81,21,520.- find out the non-reported income of Pillechan for the years 2019-20,2020-21 and 2021-22.

Let's now see how the Investigation happens in this case

EXPENDITURE THEORY

Another Method used in Investigation is the Expenditure Theory

- Expenditure theory is used to find out the Un reported Taxable income just like in Net Worth Theory
- This method is suitable when
 - There are no books of accounts maintained
 - Books of accounts are not available
 - Books of accounts/records are inadequate
 - Taxpayer is withholding records
 - Taxpayer has no assets visible or identifiable.

Sl No	Stage	Description
1	Cash in Hand	<ul style="list-style-type: none"> • Net Worth Method reports cash in hand at the year end • Expenditure method reports increase or decrease in cash in hand during a period • Cash hoard adjustment will be done here just like in Net Worth Method
2	Cash at Bank	<ul style="list-style-type: none"> • Similar to the adjustment for Cash in hand • Here the cash increase or decrease during the period is taken into consideration • Either the Book Balances or the Bank Balances are considered here • If one of Book/ Bank Balances is selected for one year, the same should be selected for the subsequent year also

Cont.

SI No	Stage	Description
3	Inventory	<ul style="list-style-type: none"> • Inventory Balances at the beginning and end are considered • The Increase or decrease in inventory is calculated by subtracting the Opening Inventory from the Closing Inventory
4	Inter Company Transfers	<ul style="list-style-type: none"> • This is normally ignored here • Initial Investment in the company is only considered here
5	Sole Proprietorships	<ul style="list-style-type: none"> • Net Changes in assets and liabilities should be reflected on the Individual expenditure schedule • Reduction for the Adjustments on account of depreciation/amortization also has to be made
6	Exchanges	<ul style="list-style-type: none"> • Payments to/ behalf of people to be classified as expenditures • Reimbursements should be classified as source of funds
7	Partnerships	<ul style="list-style-type: none"> • Total Earnings or Losses Plus any contribution less withdrawals
8	Credit Cards	<ul style="list-style-type: none"> • Net Changes in Credit Card Balances is taken into consideration
9	Other Assets	<ul style="list-style-type: none"> • Net Changes in the Assets – whether increase or decrease is taken into consideration
10	Loans	<ul style="list-style-type: none"> • Only receipt of money borrowed and total payments made during the period
11	Income and Expenses	<ul style="list-style-type: none"> • Income and Personal Expenses -based on actual disbursement
12	Deferred Gains	<ul style="list-style-type: none"> • Gains are recorded when recognized
13	Depreciation, Amortisation	<ul style="list-style-type: none"> • Not at all recognized since they do not relate to the use of funds

In this particular method, the Forensic Accountants compare the total Cash Uses to Total Income for the period. If total income is significantly lower than the total cash expenditures, there is possibly additional, undisclosed income.

Let's take an example of Mr. Thalathil Dinesan from whom the following details have been obtained for Financial Year 2022-23

Cash Sources	
Opening Bank Balance	35,000
Salary Received	8,65,000
Interest and Dividend Income	39,000
Income from Other Sources like Lottery	25,000
Rental Income	1,80,000
Total Cash Sources	11,44,000
Cash Uses	
Closing Bank Balance	65,000
Purchase of Car	8,25,000
Credit Card Payments	3,60,000
Purchase of Property	23,50,000
Purchase of Shares	10,15,000
Purchase of Jewels	8,15,000
Other Expenses	2,65,000
Total Cash Uses	56,95,000
Estimated Funds from Unknown Sources	45,51,000

In the given case, Mr. Thalathil Dinesan has income to the tune of Rs. 11,44,000 whereas the spending during the year is to the tune of Rs. 56,95,000 and the difference of Rs. 45,51,000 could be related to the Funds from Unknown Sources.

PROBLEM 2

Compute the Estimated Funds from Unknown Sources of Mr. Manavalan for the Year 2022-23 from the information furnished below

Rent Paid During the year	1,80,000.00
Salary Received During the year	8,40,000.00
Honorarium received for Motivational sessions taken	4,15,000
Holiday Trip Expenses to Thailand	4,25,000.00
Diamond Given to Mr Dharmendra on Occasion of his marriage	9,35,000.00
Credit Card Payments during the year	11,25,000.00
Bank Balances as at 01.04.2022	85,000.00
Bank Balances as at 31.03.2023	3,75,250.00

INVESTIGATION APPROACHES CAN BE DIVIDED INTO TWO-

- Investigation using Financial Data and
- Investigation using Intelligence

First let us see the Investigation using Financial Data

SI No	Stage	Description
1	Search	Investigation of the Premises of the Person-includes the visit of the premises of the person where the business is carried on and also the place where the person resides. This search mechanism would help in uncovering certain vital information as to <ol style="list-style-type: none"> a. Actual Cash in Hand b. Bank statements/other investment details held at the premises

Cont.

SI No	Stage	Description
2	Public Records	This involves accessing the records maintained at the Corporation, Village Offices etc. finding out the Properties etc. registered in the name of the person
3	Life Insurance	Life Insurance Premium Payments made by the person is also taken into consideration as this is made normally out of savings
4	Improvements to Home	This Could relate to the Purchase of <ul style="list-style-type: none"> ● Furniture and Fixtures ● Electronic appliances ● Cabinets ● Paintings ● Appliances
5	Individual Tax Returns	This is for finding the income reported during the period- There would be emphasis on the Statements available in the Income Tax Portal-including the 26AS and AIS (Annual Information Statements) There would be analysis of the Information available in the GST Portals
6	Analysis of Financial Statements of entities where the stake is held	The entities where the person holds stake would be considered, with special focus on the following <ul style="list-style-type: none"> ● No of Shares Held ● Profits/Dividends Distributed by the Concerns. ● Any Loan/ Deposit made to the Concerns. ● Related Party Transactions of the Concerns as reported.
7	Obtaining Bank Statements from the Banks	This would involve obtaining the Bank Statements directly from the Banks where the accounts are held by the person directly by the Forensic Accountant. There would be emphasis on the following <ul style="list-style-type: none"> ● Cash Deposits ● Fixed Deposits Opened During the period

Cont.

SI No	Stage	Description
8	Credit Card Statements	<p>The Credit Card Statements of the Person would be obtained- the payment for the Credit Card Transactions done during a period gets reflected in the Bank Statements but information as to the Nature of Spending will not be reflected in the Statement at all.</p> <p>Credit Card Statement analysis serves the following purposes</p> <ul style="list-style-type: none"> ● Information as to the nature of spending and also investments in any Hidden Assets. ● Credit Cards come with a credit limit which is based on the Account Turnover/Credits in account which is fixed by Financial Institutions. ● A Forensic Accountant can easily assess the person's credibility from the Credit Card Statements given
9	Analysis of the Living Expenses of the Person	<p>Living Expenses of the Person include</p> <ul style="list-style-type: none"> ● Payments for Utilities ● Payments for Insurance ● Donations, Charity etc. <p>This would also throw some light on the person's income and living standards</p>
10	Vehicles owned	<p>Analysis of the Vehicle owned does not restrict the investigation alone to the existence of the vehicle but also to ascertain the real owner and liabilities, if any</p> <p>This would include</p> <ul style="list-style-type: none"> ● Analysis of the RC copy as well as Insurance: - This would specify the Owner as well as Hypothecation Details
11	Securities	<p>Investments made in Shares and other Securities are also considered.</p> <p>This information gets reflected in</p> <ul style="list-style-type: none"> ● AIS (Annual Information Statement) – Available in the Income Tax Portal; ● Bank Statements- Dividends Credited/ Settlement from the Depository Participant, Annual Maintenance Charges Collected
12	Property Taxes	Information as to whether Property Taxes are

INVESTIGATION USING INTELLIGENCE

SI No	Stage	Description
1	Background	<p>The so-called in-depth investigation will involve</p> <ul style="list-style-type: none"> ● Analysis of the Educational Background of the Person: - Whether the person was a school/college dropout etc., Any such remarks/ incidents which would lead the forensic accountant in arriving at conclusions regarding habits, attitude, et. e.g., person would have served some months/years in juvenile home for illegal acts. ● Analysis of Family Background etc.: - Sometimes this may provide answers for the question as to why the person committed frauds-pressure from family, to meet an exigency. e.g. is the case of an employee who stole cash from the concern to meet the surgery of his father due to the sole reason he did not have funds to meet the same and later on which he made good and the investigation revealed this fact.
2	Purchase of Commodities	<p>Certain Transactions will never come within the Bank Statements, etc.-for example purchases made by Cash.</p> <p>One such case the party was seen going to a Jeweler's Shop and came back after half an hour with a big suitcase. Forensic accountant found out later that it was purchase of Gold for which cash payment was done. The same transaction was not found recorded anywhere else or the source also was not known.</p>
3.	Check on the Corporate	<p>The corporate in which the person is a director, whether the same entity had filed returns in time, whether the status of the Company is active, Disclosures within the financial statements also could be analysed.</p>
4	Companion	<p>Here, the analysis is on the spending.</p> <p>Forensic accountant would check the background of the companion-family, job, etc.</p> <p>The places of visit-Clubs, Sporting Events, Malls, Restaurants, etc. would also be considered.</p> <p>Even enquiry with friends of both these people would come within the scope of forensic accountant.</p> <p>The companion might be running a business also, like the person who is investigated and in such a case who manages that business, whether the party here is interested in that business run by the companion.</p>

Cont.

SI No	Stage	Description
5	Wiretap	<ul style="list-style-type: none"> • An eccentric mechanism but the need of the hour when it's the matter of national security or general public welfare. • Here forensic accountants would be keeping the telephone conversations under surveillance. • This would be done when they have evidence regarding critical communication and the tapping of the same assumes significance
6	Telephone records	<p>The telephone records of the customer would throw light on</p> <ul style="list-style-type: none"> • Communication with a person in Say Tax Havens or outside India where the person could be having hidden assets or Undisclosed Bank Accounts.
7	Information Requests from Banks	<p>The forensic accountant might ask for Information of the Party from Banks Like Swiss Banks and Cayman Islands Bank Authorities and the same may be furnished by the concerned Banks.</p>
8	Accountant	<p>The forensic accountant might seek information from the accountant who had filed the returns for the party.</p> <p>The accountant may or may not have possession of the entire information about the party's transactions, etc. but will have certain information which may not be disclosed in returns like property purchases, Mutual fund investments etc.</p> <p>Accountant may be filing returns for the related concerns or sister concerns which may not be disclosed elsewhere in the Financial Statements or Returns of the Party and the discussion may lead to discovery of such vital information.</p>

MULTIPLE CHOICE QUESTIONS (MCQ) FOR PRACTICE

- 1 For ascertaining the ownership and value of vehicles owned
 - a) RC Book is considered
 - b) Insurance is considered
 - c) Details from Vahan Portal is considered
 - d) All of the above

- 2 The credibility of a person is well ascertained from the (Choose the Most appropriate answer)
 - a) Life Insurance-Sum assured
 - b) Village office-Income Certificate
 - c) Credit Card-Credit Limit
 - d) Demat Account Statement

- 3 Living Expenses of a person include
1. Payment for Utilities
 2. Payment for Repair of House
 3. Investment in Shares
 4. Donations, Charity
- a) 1 Only
b) All of the above
c) 1,2 and 3 only
d) 1 and 4 only
- 4 In Expenditure theory, the excess of Cash uses over Cash sources reflects
- a) Estimated Funds from Unknown Sources
 - b) Cash inflows from operations
 - c) Net Income from Operations
 - d) Funds from Operations
- 5 Background of the person is deeply analysed in which of the following methods of investigation (Choose the most appropriate one)
- a) Investigation using Intelligence
 - b) Investigation using Financial Data
 - c) Ratio Analysis
 - d) Investigation using CAAT tools

DESCRIPTIVE QUESTIONS



- 1 Explain why the Forensic Accountant would be considered more of a bloodhound than a watchdog ?
- 2 Explain the Net Worth Theory
- 3 Enumerate the Circumstances when the Expenditure theory could be used
- 4 Explain how analysis of credit card statements help a forensic accountant during investigation
- 5 Explain Investigation using Financial Data

CHAPTER 2

LAW RELATED TO FRAUD AND FORENSIC ACCOUNTING AND INVESTIGATION STANDARDS



LEARNING OBJECTIVES

- Laws Empowering Forensic Accountants
- Forensic Accounting and Investigation Standards

2.1 LAWS EMPOWERING FORENSIC ACCOUNTANTS

The Various Laws, Regulations and Statutes in India empowering Forensic Accountants include

Companies Act, 2013

SEBI Act, 1992

Information Technology
Act, 2000

Insurance Act, 1938

Prevention of Money-
Laundering Act, 2002

Income Tax Act, 1961

Indian Penal Code

- The Companies Act, 2013
- The SEBI Act, 1992
- Information Technology Act, 2000
- Insurance Act, 1938
- Prevention of Money Laundering Act, 2002
- Income Tax Act, 1961
- Indian Penal Code



Now let us look into the salient features of the act empowering Forensic Accountants

Law	Provisions
Companies Act, 2013	<ul style="list-style-type: none"> ● Section 447 of the Companies Act deals with punishment for fraud ● There is reference to the same in Sec 7(5), 36, 75, 206(4), 213, 229, 251(1), 339(3), 448 for Directors, Key Managerial Personnel, Auditors and / or officers of the company ● Sec 7(5) deals with fraud with regards to Registration of a Company ● Sec 36 relates to inducing people to invest money ● Section 75 deals with Acceptance of deposit with intent to defraud depositors or for any fraudulent purpose ● Section 206(4) deals with conducting business of a company for fraudulent or unlawful purpose ● Section 213 deals with business Conducted with intend to defraud creditors ● Section 229 dealing with Furnishing false statement or mutilation or destruction of Documents ● Section 251(1) dealing with Application for removal of name from register with the intent of evading liabilities or intention to deceive ● Section 339(3) deals with conducting business of the company with the intend to defraud its creditors ● Section 448 deals with making a false statement in any return, report, certificate, financial statement, prospectus, statement or document.
SEBI Act, 1992	Regulation 11C of the SEBI act empowers SEBI to direct investigation of the affairs of the intermediaries or brokers whose actions are detrimental to the interests of the investors
Information Technology Act, 2000	<p>Section 43 and 44 of the Information Technology Act lays down penal provisions for</p> <ul style="list-style-type: none"> ● Unauthorised Copying of data ● Unauthorised Access and downloading files ● Introduction of Virus or malicious programmes ● Providing assistance to any person to facilitate unauthorised access ● Damage to a computer system or computer network ● Denial of access to authorized persons

Cont.

Law	Provisions
Insurance Act, 1938	Section 33 lays down provisions for IRDA (Insurance Regulatory and Development Authority to direct investigation into the affairs of any insurer
Prevention of Money Laundering Act ,2002	Section 3 -Direct or indirectly attempting to indulge or knowingly assist or is involved in process or activity connected with proceeds of crime shall be guilty of the offence of Money Laundering
Income Tax Act, 1961	<p>Income Tax directly does not speak about corruption but has a handful of provisions pertaining to the money received through ill means.</p> <ul style="list-style-type: none"> ● Section 68: - Cash Credits – Sum credited in the books of the assessee for which assessee has no satisfactory explanation or no explanation is given, same shall be charged as income ● Section 69: - Unexplained Investments: - Assessee has made investments and the same is not recorded in books and assessee has no explanation/ no satisfactory explanation about the nature and source of investments - same shall be deemed to be the income ● Section 69A: -Unexplained Money: - Assessee is found to be owner of money, bullion, jewellery or valuable article not recorded in books and there is no explanation or satisfactory explanation of the nature and source of acquisition, same shall be deemed to be the income ● Section 69C: -Unexplained Expenditure: - Assessee has incurred any expenditure books and there is no explanation or satisfactory explanation of the nature and source of acquisition, same shall be deemed to be the income
Indian Penal Code	<ul style="list-style-type: none"> ● Section 168 - Public Servant engaging in Trade ● Section 171B -Bribery ● Section 403-Dishonest misappropriation of Property ● Section 405-Criminal Breach of Trust ● Section 417-Cheating ● Section 463-Forgery

2.2 FORENSIC ACCOUNTING AND INVESTIGATION STANDARDS (FAIS)

- FAIS seeks to provide the minimum standards for undertaking Forensic Accounting and Investigation (FAI) Engagements

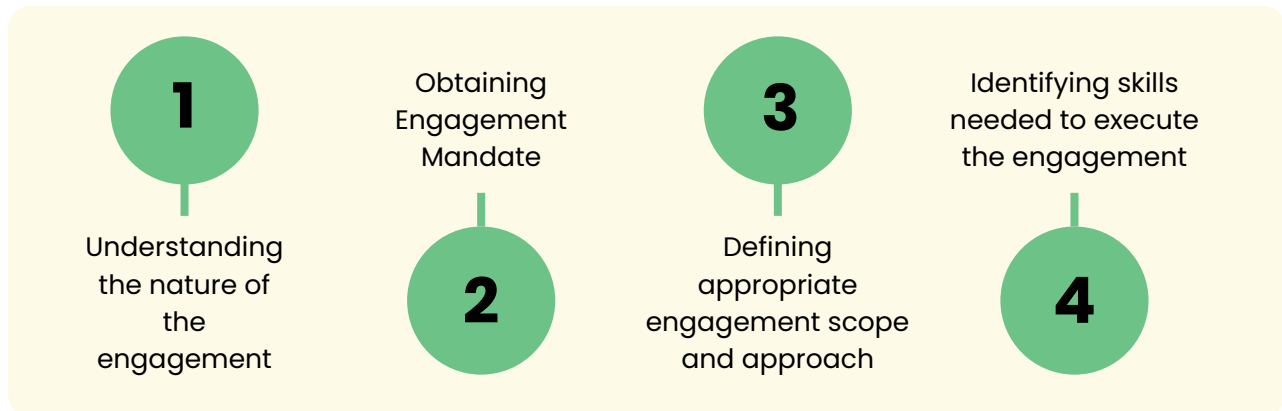
Following are the Forensic Accounting and Investigation Standards

No	Standard
FAIS 110	Nature of Engagement
FAIS 120	Fraud Risk
FAIS 130	Laws and Regulations
FAIS 140	Applying Hypothesis
FAIS 210	Engagement Objectives
FAIS 220	Engagement Acceptance and Appointment
FAIS 230	Using the work of an Expert
FAIS 240	Engaging with Agencies
FAIS 250	Communication with Stakeholders
FAIS 310	Planning the assignment
FAIS 320	Evidence and Documentation
FAIS 330	Conducting Work Procedures
FAIS 340	Conducting Interviews
FAIS 350	Review and Supervision
FAIS 360	Testifying before a Competent Authority
FAIS 410	Applying Data Analysis
FAIS 420	Evidence Gathering in Digital Domain
FAIS 430	Loans or Borrowings
FAIS 510	Reporting Results
FAIS 610	Quality Control

Let's have a detailed discussion on the Standards

2.2.1 FAIS 110: – NATURE OF ENGAGEMENT

- Objective of the standard is to assist the professional in
 - Understanding the nature of the engagement
 - Obtaining Engagement Mandate
 - Defining appropriate engagement scope and approach
 - Identifying skills needed to execute the engagement



- Guidance note provides illustrations and examples to help professional decide on the nature of engagement and whether it comes within purview of Forensic Accounting.
- It even distinguishes Forensic accounting and Investigation as different things by stating that if the objective is gathering evidence for presenting before competent authority it may be a Forensic Accounting engagement and if the objective is just to uncover a fraud it may be just investigation.

2.2.2 FAIS 120: – FRAUD RISK

Identifying most vulnerable areas

Performing a preliminary fraud risk understanding of the areas

Identify and prepare a list of fraud risk indicators

Prioritise the work procedures and allocate them to the people based on their skills

- Objective of this Guidance Note is assisting the professional in
 - Identifying most vulnerable areas
 - Performing a preliminary fraud risk understanding of the areas
 - Identify and prepare a list of fraud risk indicators
 - Prioritise the work procedures and allocate them to the people based on their skills.

- Guidance note even sets out the Various fraud risk indicators, called as Red Flags, Risk in relation to expenses and vendor onboarding, Risk in relation to loans
- Guidance note even throws light on the Fraud Triangle aspect- Opportunity, Incentive and Rationalisation which are the elements which should co-exist for a fraud to happen

2.2.3 FAIS 130:- LAWS AND REGULATIONS

- Objective is to ensure that the professional has knowledge of laws and regulations so that it serves the desired objectives of authorities
- Laws here can be classified into:
 - Direct impact laws-E.g., Evidence Act, Money Laundering Act
 - Engagement specific laws-E.g., Insolvency and Bankruptcy
- Guidance note also provides insight into the Laws which may be applied during Forensic Accounting and Investigation engagements- The Indian Evidence Act, 1872, The Indian Penal Code 1860, Information Technology Act 2000, Companies Act, 2013, Prevention of Money Laundering Act, 2002, Prevention of Corruption Act, 1988, Sarbanes Oxley Act of 2002, etc.

2.2.4 FAIS 140:- APPLYING HYPOTHESIS

- Hypothesis gives direction to engagement and would make the evidence collection more methodological and effective
- Hypothesis would be formed once the understanding of the background of the case is obtained
- A generic suggestive practical approach would be as follows as depicted in the image below



- Work procedures to be followed to ascertain the existence of debtors as indicated in Guidance Note Include
 - Asking for Balance Confirmations
 - Conducting site visits of Trade receivable holders to check their existence
 - Perform the Public Domain Checks

NOW LET’S TAKE UP THE STANDARDS ON ENGAGEMENT MANAGEMENT

2.2.5 FAIS 210: –ENGAGEMENT OBJECTIVES

- This standard seeks to ensure that there is clarity regarding the scope of engagement and the expected outcome is in line with the proposed objects of the assignment
- Understandings of the scope to be inculcated in the letter called “Engagement Acceptance and Appointment”
- Approach for setting the objectives would be
 - Identify the purpose of the engagement
 - Determining the stakeholders involved
 - Consider the legal or administrative context
 - Identify the goals and outcomes
 - Communicate the purpose of engagement

2.2.6 FAIS 220: – ENGAGEMENT ACCEPTANCE AND APPOINTMENT

- It mandates the undertaking of due diligence while evaluating terms and conditions of appointment
- While undertaking an assignment
 - Risk Parameters are to be ascertained
 - Official Engagement letter is to be obtained
 - Engagement risks are to be evaluated
 - Changes/additions to scope after commencement of engagement is to be made in writing
 - Understanding of Key Stakeholders, both direct and indirect are to be done.

2.2.7 FAIS 230: USING THE WORK OF AN EXPERT

- Conveys the fact that there would be circumstances wherein services of an expert would be required but the ultimate responsibility shall remain with the Forensic Accountant
- Need of an expert would arise
 - When neither of team members possess the requisite skills in a particular area, say valuation of oil well
 - Gathering Evidence through electronic media
 - Legal advice
 - Analyses of Trades etc.

- While engaging the expert
 - o Understand the expert
 - Knowledge of expert’s qualifications is needed
 - Previous Works of expert also to be evaluated
 - Discuss with other people who have engaged the expert
 - Resources written or published by expert
 - o Define the Scope and Deliverables
 - Objective and Scope of work
 - Responsibilities of Expert
 - Confidentiality Requirements
 - Reporting Deadlines and to whom reporting is to be done
 - o Evaluate the Work done
 - Sources and Information used
 - Assumptions used
 - Chances of Conflict of Interest in the work done also to be evaluated

2.2.8 FAIS 240: - ENGAGING WITH AGENCIES

- Applicable when the expert is appointed by an agency
- Expert has to
 - o Get a clarity on the terms of the engagement
 - o Understand the legal and regulatory requirements behind the engagement
 - o Maintain documentation and also other protocols
- Agencies might control the process of gathering of evidence and the professional has to rely on such information. In such a case, the same must be disclosed in line with FAIS 510 on “Reporting Results”

2.2.9 FAIS 250: - COMMUNICATION WITH STAKEHOLDERS

This standard lays down guidelines for

- Clear, Continuous and two-way communication with several stakeholders needed at various stages of Forensic Accounting and Investigation assignment
- Communication has to be done maintaining protocols
- Essential and Significant matters are communicated
- Good Etiquette and Confidentiality has to be maintained throughout

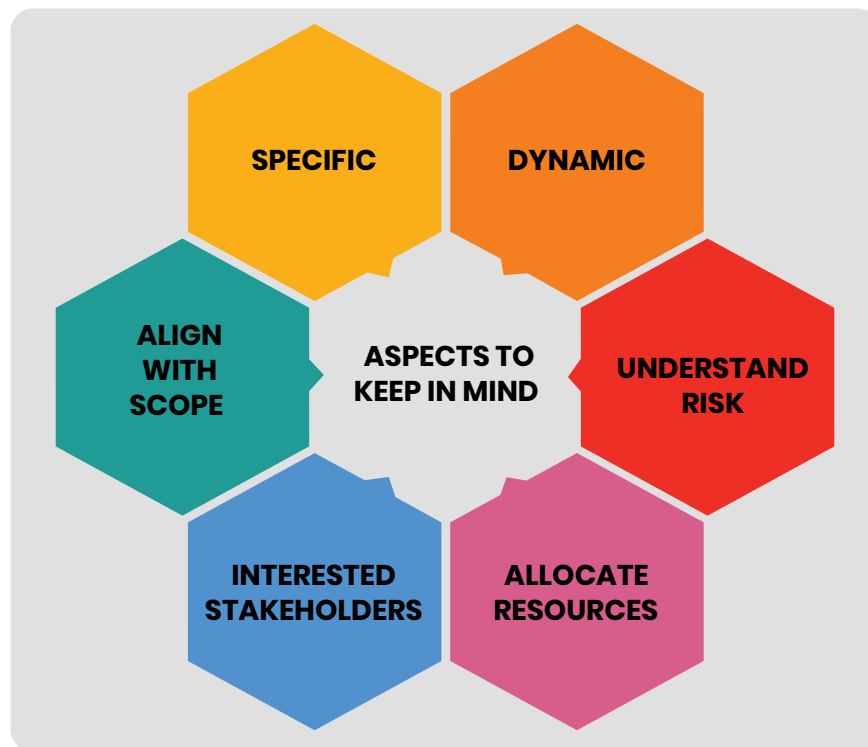
Procedures for ensuring Good Communication

- List of Stakeholders to be made, who will communicate with them to be decided
- Stakeholder list to be dynamic as there would be more people added to list or deleted from list as the engagement progresses
- Form and Format of communication- Oral, verbal, Voice recordings etc.
- When expert is engaged, should consider FAIS 230 ON “Using the work of an Expert”

- Stakeholders vary from Organisation to organisation and from circumstance to circumstance and so would be the communication also
- If Primary Stakeholders are engaged in Fraud, then the professional has to revise the stakeholders to whom the communication has to be made

2.2.10 FAIS 310: -PLANNING THE ASSIGNMENT

- Professional to have a well-made plan for the assignment
- Planning to be conducted in a process driven manner, undertaking key activities and communicating the same
- Procedures would include developing a checklist
- While dealing with a complex assignment, professional need to allocate ample time for gathering information, interviews and doing analysis
- Depth of Planning should be based on the nature of engagement -Like Financial Statement Fraud, Corruption or Asset Misappropriation
- Planning also depends on familiarity with the stakeholders



- Aspects to be kept in mind
 - o Specific:- focus on the subject matter
 - o Dynamic:- Plans need to be revised depending on the situations
 - o Plan can be aligned with scope of the engagement
 - o Understand the risks and incorporate them in the plan formulation
 - o Identify interested stakeholders
 - o Allocation of resources based on needs of the engagement

2.2.11 FAIS 320:- EVIDENCE AND DOCUMENTATION

- Forensic Accounting and Investigation Assignments probably extend to court-rooms and therefore the evidences gathered assume significance and FAIS 320 throws light on such evidence collection.
- Evidences can be classified into
 - Primary Evidence:- Original Documents
 - Secondary Evidences:- Certified Copies of Original Documents
- Another classification of Evidence being
 - Oral Evidence: - gathered during interview or enquiry
 - Documentary evidence:-includes records in the form of documents like Invoices, Orders
 - Electronic Evidence:- records kept in electronic or digital mode
- The third classification of evidence being:-
 - Technical Evidence -generated from Mechanical devices like Electronic meter
 - Camera Evidence:- Photographs or images of the subject matter
- The type of evidence would determine the manner in which it is to be gathered
- While gathering evidence, maximum amount of evidence is to be collected
- If evidence is collected with the help of expert, additional safeguards are to be taken as per FAIS 230 "Using the work of an expert"
- Professional has to verify the original and obtain copies of the same
- Non Co-operation from stakeholder in gathering evidence is to be reported to primary stakeholder and the same should be stated in the report also
- All original documents obtained to be kept in a sealed cover or lock and key
- Preserve the evidence till the conclusion of all legal proceedings



2.2.12 FAIS 330: - CONDUCTING WORK PROCEDURES

- Designing work procedures based on the scope and objectives of the assignment
- A phased approach is effective
 - Phase 1 :- Focus on data collection and evidences
 - Phase 2 :- Through Interviews and Interactions with stakeholders
- Assignment should be carried out in a meticulous manner
- While finalizing work procedures, the following information may be sought
 - Confirm initial understanding of issues
 - Prepare timeline of events
 - Understand financials and substantial events
 - Perform Financial Analysis
 - Understand Red Flags

2.2.13 FAIS 340: -CONDUCTING INTERVIEWS

- Considerations a professional should have while conducting Interviews in a Forensic Accounting and Investigation assignment
- Objectives of Interview and role of interview is to be understood before the interview
- Interview to be done only after the information gathering process is complete pertinent to the interview
- Objective of Interview is
 - Validate existing facts
 - Seek additional information
- Participants of Interview
 - Interviews normally done with the help of an interview team
 - Roles and Responsibilities to be clearly defined among team members
 - A questionnaire outline would give a good structure to the interview
 - A Mock interview would be a better option to prepare for the same
 - Co-Interviewer can supplement the main person and can take notes
 - An Interpreter would also serve the purpose of a good interview
- Location of Interview
 - Location should be conducive for the interview
 - Interview should be during Business hours
 - Availability of amenities should also be ensured
 - Interviews to be conducted with privacy considerations also
- Only one person to be interviewed at a time, presence of multiple interviewee will influence the other person's responses.
- Standard also lays down how to carry out an interview -opening an interview, note taking, confidentiality, questions to be asked during an interview and closing an interview

2.2.14 FAIS 350: –REVIEW AND SUPERVISION

- Directing the efforts of the engagement team to ensure objectives are achieved as planned
- Work procedures are performed effectively and efficiently in line with the terms of engagement
- Work performed by team member may be periodically evaluated to find out whether the same was adequately performed
- Ensure that the documentation is appropriate
- Extent of supervision depends on
 - Nature of Company and its size
 - Nature of assigned work
 - Knowledge, skill of each team member
 - Nature, size of data
- Purpose of review is
 - Work procedures are satisfactory
 - Documentation is proper
 - Outputs/Deliverables are clear, objective, factual
 - Services are performed as per the terms in the engagement

2.2.15 FAIS 360:- TESTIFYING BEFORE A COMPETENT AUTHORITY

- Professional may be called upon by competent authorities to testify on evidence gathered
- Requirements of the standard
 - Compliance with Principles of FAIS
 - Extend paramount duty towards competent authority
 - Focus on testifying the evidence gathered only
 - Devote time for preparing and testifying
- Procedures
 - Primary duty is towards the competent authority-i.e. Courts and not towards the Stakeholder which had appointed the professional
 - Scope of testimony shall be restricted to facts gathered during the assignment
 - Testimony shall be given in an impartial and professional manner
 - Adequate documentation of records to be presented during testimony should be made ready
 - Provide an Impartial Testimony before the authorities

2.2.16 FAIS 410:-APPLYING DATA ANALYSIS

- Professional to Understand the Technical aspects of Data Analytics and deploy the evidence gathering power
- Standard seeks to provide professional with information, approach and illustrations to assist in developing application of data analytics techniques in an Forensic Accounting and Investigation engagement

- Procedures
 - Data Analysis Plan:-Understanding of Data would enable the professional to develop a Data Analysis Plan (DAP) for the Forensic Accounting and Investigation engagement
 - Depending on the engagement, what is to be included in DAP shall be decided
 - Data preparation for the data analytics should include data acquisition and validation
 - Data Analysis and reporting:-Execution of all critical data analysis identified in Data Analysis Plan is done here
 - Data Preservation:-This is needed as the result of data analysis would have to be produced in court
- Some of the commonly known advanced tools available for Data Analysis include Knime, ACL, IDEA, SQL, SAS, Python
- During data analysis tests, professional might get trends relevant to the entire engagement and may revise the tests if needed
- Depending on the nature of analysis, output may be presented in format understandable to the recipient
- Professional shall also consider the FAIS 130 on Laws and Regulations while carrying out the tests
- Professional might use unstructured data for the analysis also
- Since Forensic Accounting and Investigation engagements are dynamic in nature, FAI professional may exercise the judgement while applying data analysis

2.2.17 FAIS 420: EVIDENCE GATHERING IN DIGITAL DOMAIN

- Guidance to the Professional for the gathering of electronic evidence in the digital domain ensuring that it satisfies requirements of judiciary
- Professional should have a well planned approach while seeking to gather evidence in the Digital Domain. Professional should have understanding of the Information Systems, e-gathering exercise should be carried out in a successful way
- Applicable legal environment for the Digital Evidence and Cybercrimes should also be considered -including Indian Evidence Act, Information Technology Act, Code of Criminal Procedure, Indian Penal Code, Bankers Book of Evidence Act, 1891
- Professional to use judgements in ensuring the way in which the digital evidence is used
- Procedures
 - Organisation's IT environment should include -Email, ERP (Enterprise Resource Planning) System, Customer Relationship Management (CRM) System, Management Information System (MIS), Financial Accounting System, etc and a professional should have an understanding of the same
 - Understanding risk factors
 - Use of timelines, and documented procedure
 - Technical and other Regulatory Considerations

2.2.18 FAIS 430:-LOANS OR BORROWINGS

- Related to Disputed Transactions of Loans or Borrowings
- Understanding circumstances that lead to dispute and whether there is any merit for this dispute
- Procedure
 - o Understanding of nature of loans or borrowings –documents for review will include – Loan application, project reports, loan sanction letter
 - o Additional sources like Compliance submissions with the regulator, Registrar of Companies
 - o Understand the objectives of the engagement like Violation of legal, contractual or regulatory provisions, etc.
 - o Professional may be required to develop hypotheses as per the nature of engagement

2.2.19 FAIS 510:- REPORTING RESULTS

- Mandates on a written report comprising of the findings along with the evidence relied upon by the professional in a structured manner
- Objective of the report is to make stakeholders understand the case, evidence helping them to reach a factual conclusion
- Procedures
 - o When drafting a report professional has to ensure that it has clarity, is accurate and it meets the assigned objectives
 - o Reporting requirements may vary from assignment to assignment
 - o Key elements of a report include
 - Covering Letter
 - Executive Summary
 - Title, addressee and distribution list
 - Scope and Objectives of assignment
 - Approach and broad work procedures written
 - Reference as to the use of the expert
 - Reference to FAIS or other standards
 - Detailed Findings
 - Assumptions, limitations and disclaimers
 - Conclusions
 - o Standard also lays down considerations for issue of interim reports and also the situations where the professional would not be able to complete the report
 - o The report has to satisfy certain attributes as laid down
 - Free from Bias
 - Factual
 - Clear and Unambiguous
 - Transparent
 - Chronological
 - Meeting the objective
 - Restricted Circulation

2.2.20 FAIS 610: - QUALITY CONTROL

- Practical application of Quality control measures to ensure that there is quality in work performed
- Procedures
 - o Check whether basic checks are in place. These include
 - Independence Check -By reviewing past and current business and professional relationships
 - Obtaining understanding of the engagement
 - Engaging the services of an expert when the professional feels it is necessary
 - Discussion with the client to understand the nature and scope of the assignment
 - o Continuous monitoring of work to be done throughout the assignment
 - o Plan may need revisions depending on the work
 - o Market Surveys or field studies would be needed in course of the assignment
 - o Quality Control review:- Before closing the report, Professional may perform an independent internal review which may be in the form of peer review
 - o Professional may build a system of safe filing, storage and retrieval of all working papers



MULTIPLE CHOICE QUESTIONS (MCQ) FOR PRACTICE

- 1 As per Section_____ of the Insurance Act, 1938 IRDAI can direct investigation into the affairs of an insurer
- 31
 - 32
 - 33
 - 34
- 2 Section 69C of the Income Tax Act,1961 Covers
- Unexplained Expenditure
 - Unexplained Money
 - Unexplained Investments
 - Cash Credits
- 3 FAIS 140 Deals with
- Applying Hypothesis
 - Engaging with Agencies
 - Conducting Interviews
 - Review and Supervision
- 4 Extent of Supervision as per FAIS 350 Depends on
(Choose the most appropriate answer)
- Nature of Company and its size
 - Nature of assigned work
 - Knowledge, skill of each team member
 - Nature, size of data
- 1,2,3 and 4
 - 1,2 and 3
 - 1 and 2 Only
 - 2 and 3 Only
- 5 As laid down in FAIS 360 when the Testification happens before a competent authority
(Choose the most appropriate answer)
- Primary Duty is towards the Stakeholder who has appointed the Forensic Accountant
 - Primary Duty is towards the Entity for whom the assignment is carried out
 - Primary Duty is towards the Competent authority to whom the Testification happens
 - Primary Duty is towards the Top Management of the entity for whom assignment is carried out

**DESCRIPTIVE QUESTIONS**

- 1 Explain the Procedures for ensuring good communication as laid down in FAIS 250
- 2 What are the different aspects to be kept in mind while planning a Forensic Accounting and Investigation assignment as per FAIS 310
- 3 What are the key elements of a Forensic Accounting and Investigation Report
- 4 Enumerate Various Provisions of the Companies Act, 2013 empowering Forensic Accountants
- 5 Explain the Classification of Evidence as laid down in FAIS 320

CHAPTER 3

FINANCIAL TRANSACTIONS AND FRAUD SCHEMES



LEARNING OBJECTIVES

- Financial Statements
- Financial statement frauds
- Objectives behind financial statements frauds
- Schemes of financial statements frauds
- Warning signs or red flags in financial statement frauds
- Fraud schemes

3.1 FINANCIAL STATEMENTS

- A Collection of reports
- About an organisation's Financial results for a particular period
- About the financial condition of business at a particular point of time
- About cashflows of the organisation during a particular period
- Containing full and proper disclosures of significant facts and information

3.2 FINANCIAL STATEMENT FRAUDS

- Deliberate misrepresentation of data and information in Financial Statements with an intent to misled the user and thus creating a wrongful impression of financial health.



3.3 OBJECTIVES BEHIND FINANCIAL STATEMENT FRAUDS

- To make performance better than actual (to entice investments and loans)
- To make performance look worse than actual (to lower the tax liabilities)

3.4 PERPETRATORS OF FINANCIAL STATEMENTS FRAUDS

- Normally perpetrated by the upper management as the Financial Statements are created at the management level

3.5 SCHEMES OF FINANCIAL STATEMENTS FRAUDS

TYPES OF FINANCIAL STATEMENT FRAUDS

Time Manipulation

Entry Falsification

Non-disclosure or improper disclosure of facts

- Time Manipulation
- Entry Falsification
- Non-disclosure or improper disclosure of facts

Let's now discuss each of these in detail

3.5.1 TIME MANIPULATIONS

- Early recognition of revenue
- Postponement of expense

Early Recognition of Revenues

Recording a sale pending supply

- Recording sale pending finalisation
- Recording a sale even when sent on consignment
- Recognising in full the activation fees without amortisation
- Recording revenue in multiple element contract where there is undelivered element of supply



Postponement Of Expenses

- Recording of expenses only on payment and not on accrual basis
- Large revenue expenses are capitalized
- Higher amortization period than appropriate
- Showing higher useful life of fixed asset than appropriate thereby reducing the charge of depreciation

3.5.2 ENTRY FALSIFICATION OR ENTRY MANIPULATION

- Fictitious revenues
- Manipulation of liabilities and expenses
- Manipulation of values of fixed assets

Fictitious Revenues

- Manufacture of transactions that appear to be sales
 - Fictitious sale to existing customers
 - Fictitious sale to fictitious customers
- Classifying other receipts as sales
 - Insurance claims
 - Sale of fixed asset
 - Purchase returns etc

Manipulating Liabilities and Expenses

- Showing short term liability as long term or vice versa
- Capitalisation of current expenses to fixed asset
- Old book debts still carried in books
- Writing of liabilities to income
- Adjusting expenses against reserves
- Non recognition of liabilities for unpaid expenses though incurred

Manipulating the Value of Asset

- Inventory valuation at higher price than actual for correct quantity
- Inventory valuation at higher quantity than actual for correct rate
- Classifying long term investment as short term investment
- Non adjusting fall in investments value
- Capitalising revenue expenses to fixed asset
- Investment in sister companies classified as advance to other parties

3.5.3 NON DISCLOSURE OR IMPROPER DISCLOSURE

- Liability omissions: - Non disclosure of loan covenants or contingent liabilities.
- Events occurring after the balance sheet date: - Avoid judgements of courts etc.
- Management frauds – non disclosure
- Related party transactions: - Self dealing if not at Arm's Length Price

- Accounting changes: – Change in accounting principles, estimates and reporting entities

Example: Purchase of raw materials from sister company at lower rate and sale of finished product to another sister company at higher rate is a case of artificial profit building and falls under Related Party Transactions.

3.6 WARNING SIGNS OR RED FLAGS IN FINANCIAL STATEMENT FRAUDS

- Single person dominance in management
- Ineffective communication
- Recurring negative cash flows
- Restriction on auditors' access to people and/or information
- Rapid growth of profitability as compared to peers.
- Highly complex transactions particularly those close to period end
- Significant related party transactions not in the ordinary course of business
- Significant bank accounts or branch operations in tax holiday zones with no clear business connections
- History of violation of laws and regulations
- Attempts to justify inappropriate accounting
- Unusual growth in days sales in receivables
- Sales recorded at headquarters which do not do direct sales
- Frequent wrong classifications
- Unusual financial ratios
- Consistent higher liabilities than assets

3.7 FRAUD SCHEMES

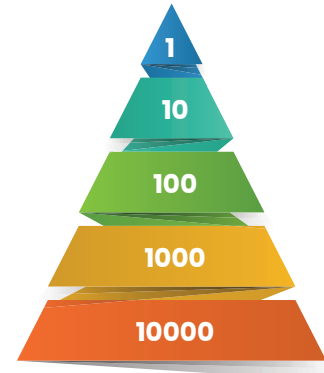
3.7.1 PONZI SCHEMES

- These refer to the investment schemes that promise to pay relatively high rates of returns for fixed term investments.
- They are fraudulent investment plans – the money that is collected is not invested at all !
- The Scheme has no legitimate source of revenue or profits to pay “returns” to investors.
- Instead, every new investment is used to pay off earlier investors.
- For e.g. if A invests Rs.1,00,000 and the return promised is 20%, when another investor B invests Rs.1,00,000 A would be paid Rs.120,0000 using the contribution of A.
- When the scheme is no longer able to attract new investors, it would collapse, and even the principal amount itself would not be paid
- In India, one such common scam was Anubhav Plantations which promised high returns for people who invested in planting teak during the period 1992–1998.It collapsed in 1998 leaving around 31,000 depositors defrauded and the amount being more than Rs.10,700 Crores
- Saradha Chit Fund scam and Sanjivani Credit Cooperative Society are the other notable ones in the list with same modus operandi



3.7.2 PYRAMID SCHEMES

- It relies on promising unrealistic returns from imaginary investments.
- Early Investors are paid handsome returns which in turn prompts them to recommend the scheme to others
- Once the new investors stop coming in, the pyramid collapses
- Investors at each stage here, charge a fee called initiation fee, which is paid by next layer of investors—a portion of the same is paid to the ones at the top layer, when there are no further new investor this stops



- E.g., the Amway Scam - Amway was accused of running this scam in the country -they had sold FMCG (Fast Moving Consumer Goods) Products at exorbitant prices-general public were more victims as they purchased these products at extremely high prices and in turn became members of the company.

- Similar on the lines was Speak Asia Online limited which did ask its investors to pay Rs 11,000 and fill up online survey forms to earn Rs 52,000 a year. Additional rewards were promised for those who could add more people into the scheme. Finally, the scammers absconded with Rs 2,276 crore from 24 lakh investors.



3.7.3 DIGITAL BANKING AND CREDIT CARD FRAUD

- Phishing attacks, identity theft, and fraudulent transactions using stolen card details are the common schemes prevalent in this form of fraud

3.7.4 MONEY LAUNDERING

- It is the process of Illegally concealing the origin of money, usually obtained from illegal activities, like smuggling etc.
- This is converted into a form that makes it seem legitimate income
- Two cases worth noting which happened in India in the recent past
 - o ICICI Bank-Videocon Case



- After a thorough investigation, the investigating authorities found out Chanda Kochhar, the then MD and CEO of ICICI Bank- had sanctioned loans worth 1,875 crores from ICICI Bank to Videocon Group.
- This was in turn returned by Videocon Group by investing in NuPower Renewables Private Limited (NRPL), a company owned by Chanda Kochhar's husband, Deepak Kochhar

o Yes Bank- DHFL case



- Case had Mr. Rana Kapoor, the founder and CEO of Yes Bank and the promoters of Dewan Housing Finance Limited (DHFL) - Kapil Wadhawan and Dheeraj Wadhawan
- Yes Bank had bought debentures worth 3,700 crores between April 2018 and June 2018 from DHFL.
- DHFL sanctioned a loan of 600 crores to DOIT Urban Ventures Pvt. Ltd. (DUVPL), which was owned by Rana Kapoor and his family.

3.7.5 STOCK MARKET MANIPULATION



- Activities like price rigging, spreading false information, insider trading are many such activities through which the fraudsters manipulate the share prices
- E.g.-Satyam Computers was one such case wherein the promoters manipulated financial statements to manipulate the share prices

3.7.6 BANK FRAUDS

- Bank Frauds can take several forms- it could be done by people within the Bank-Bank Staff and also could be done by the customers
- Even Frauds have gone to such an extent - A Duplicate Branch of State Bank of India in Panruti - which operated for almost 3 months and the fraud came to light when the customer of the fake Bank Branch discusses the same with Manager of an existing original State Bank of India Branch.

3.8 DETECTION AND/OR PREVENTION OF FINANCIAL STATEMENT FRAUD

- Tone at the top- strong ethics and strictness
- Effective whistle blower programme
- Question financial results that are always on targets
- Question about changes in auditors
- Have skeptics on the board of directors
- Question extraordinary or complex transactions
- Analyse accounts receivables-relative size factor analysis
- Question the mismatch of cash generation with revenue
- Analysis of swing in assets and/or liabilities

MULTIPLE CHOICE QUESTIONS (MCQ) FOR PRACTICE

- 1 The Fraud Scheme where the money collected from the new investors are used for paying the old investors is (Choose the Most Appropriate Answer)
 - a) Pyramid Scheme
 - b) Ponzi Scheme
 - c) Money Laundering
 - d) Deposit Scheme

- 2 A Fraud Scheme wherein Investors at each stage, charge a fee called initiation fee, which is paid by next layer of investors—a portion of the same is paid to the ones at the top layer and a portion is given to them is known as
 - a) Pyramid Scheme
 - b) Ponzi Scheme
 - c) Money Laundering
 - d) Deposit Scheme

- 3 Commonly used Forensic Accounting Softwares include all except
 - a) Caseware Idea
 - b) Zaubra Corp
 - c) Ocrolus
 - d) Fraud Finder

DESCRIPTIVE QUESTIONS

- 1 Explain Ponzi Schemes
- 2 Explain Entry Falsification or Entry Manipulation in relation to Financial Statement Frauds
- 3 Enumerate on various Red Flags in the Financial Statements

CHAPTER 4

FORENSIC ACCOUNTING – DATA SOURCES FROM DIFFERENT WEBSITES



LEARNING OBJECTIVES

- Commonly Used Forensic Accounting Softwares
- Various Data Sources for Forensic Professionals
 - Credit Information Reports
 - MCA Portal
 - GST Portal
 - Other Sources
 - Ratio Analysis
 - Google
 - Zauba Corp
- Some Fraudulent Activities carried out by corporates

4.1 COMMONLY USED FORENSIC ACCOUNTING SOFTWARES

Forensic Accounting Softwares Commonly used include

- ScanWriter
- CaseWare IDEA
- Ocrolus
- Fraudfindr
- Nunix Investigate
- Valid8
- Strongbox

4.2 VARIOUS DATA SOURCES FOR FORENSIC PROFESSIONALS

- Credit Information Reports

4.2.1 CREDIT INFORMATION REPORTS

- Credit Information Reports Available Online
 - Credit Information Reports could be used by Forensic Professionals to ascertain the credit worthiness of a person
 - Credit Scores, normally given by the Credit Investigation Agencies are used by Bankers before sanctioning loans
 - Commonly used Reports include CIBIL, CRIF, Fitch etc.
 - This Credit score is arrived at based on the past credit history of the party
 - This would help a Forensic Accountant in predicting the future of loan accounts– these reports would reflect whether the loans taken are presently classified as Standard, Substandard.

- o This could be even used while ascertaining Net Worth of persons and it even helps a person carrying out statutory audit.
- o A specimen of CRIF Report generated is given below
 - Name of the Customer
 - Constitution
 - Class of Activity
 - PAN
 - UDYAM reg no
 - GST Registration No
 - Score
 - Description also given as to what exactly the score is telling-whether the account is a high risk account, whether operations are normal, whether there is presence of delinquency in the past, etc.
 - Moreover these reports give the entire credit history of the party- loans taken since inception, even the ones which have been closed along with live and currently running ones appear in the list.



COMMERCIAL ACE TM REPORT

Order Ref ID: 8292591

Prepared For:

Application ID: -

Date of Request: 30-07-2023

Date of Issue: 30-07-2023

Inquiry Details

Borrower Details

Name:	INDUSTRIES	Short Name:	
Legal Constitution:	PROPRIETORSHIP	Applied Amount:	50,00,000
Class of Activity:	OTHER COMMUNITY, SOCIAL AND PERSONAL SERVICE ACTIVITIES	PAN:	
Applied for:	WORKING CAPITAL LOANS	UDYAM NO:	
CIN/LPIN:		CKYC:	
Phone #:		Email ID:	
Address(es):	Registered:	GSTN:	
	Other Address 1:	GSTN:	
	Other Address 2:	GSTN:	

CRIF HIGH MARK SCORE(S):

SCORE NAME	SCORE	DESCRIPTION
PERFORM COMMERCIAL 2.0	372 <small>Score Range: 300-900</small>	L-Very High Risk

Tip: A-D: Very Low Risk; E-G: Low Risk; H-L: Medium Risk; J-K: High Risk; L-M: Very High Risk; N-T: Exclusion Codes

Borrower Summary

Lender#	Total Accts#	Live Accts#	Delinquent Accts# *	Sanctioned Amt *	Outstanding Amt *	Overdue Amt *	PAR *(90+)
Your Institution							
1	17	0	5	2.6 (77.61%)	1.68	0.05	0.0
Other Institution							
2	2	1	0	0.75 (22.39%)	0.59	0.0	0.0

* Only for CRIF accounts

Length of Credit History: 10 (Yrs) / 1 (Months) Profile in Last 12 Months >>> New Accts: 7 Closed Accts: 7 New Delinquent Accts: 0

Delinquent Accts (90+): 0 days or reported as Non-Standard
(It represents percentage of total banking accounts)

Public Search of Trademark

Notices Under Section 248(2)

SINGH	24/06/2	-	
TAM	24/06/2	-	

Export To Excel **Print**

The report even throws light on the status of account for the past one year—a detailed view on the present status of the applicant – Diagram below depicts the same

COMMERCIAL ACE REPORT

CRIF HIGH FINANCE
Together to the next level

Order Ref #: -
Prepared For: -
Application ID: -
Date of Request: 30-07-2023
Date of Issue: 30-07-2023

1 Loan Terms For: Applicant as Borrower Info. as of: 30-06-2023

DETAILS

Type: Cash Credit -In INR
DPD/Asset Classification: SPECIAL MENTION ACCOUNT-2
Sanctioned Date: 26-06-2004

Lender: -
Last Payment Date: -
Current Balance: -

Account #: -
Amount Overdue: 0
Sanctioned Amount: -

Closure Reason: -
Closed Date: -
Drawing Power: -

Account Remarks: -

Current Balance History (12 Months):

	January	February	March	April	May	June	July	August	September	October	November	December
2023	00.01	00.01	00.02	xxx/xxx	00.72	43.8	--	--	--	--	--	--
2022	--	--	--	--	--	--	--	01.86	00.01	01.79	00.00	00.07

Payment History/Asset Classification:

	January	February	March	April	May	June	July	August	September	October	November	December
2023	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx
2022	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx
2021	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx
2020	--	--	--	--	--	--	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx	xxx/xxx

Suit Filed & Willful Default

Suit Filed Status: -
Suit Amount: 0
Date of Suit: -

Suit Reference: -
Willful Defaulter: Not Willful Defaulter
Willful Default As On: -

4.2.2 INFORMATION IN PUBLIC DOMAINS

These refer to the information that is easily accessible and there is no registration or payment of any fees required to access the same, Here lets some of such information which is vital for a Forensic Accounting/Investigation.

4.2.2.1 MCA Portal

Ministry of Corporate Affairs
EMPOWERING BUSINESS, PROTECTING INVESTORS
REGULATOR • REGISTRATOR • FACILITATOR • EDUCATOR

Home About MCA Acts & Rules My Workspace My Application MCA Services Data & Reports E-Consultation Help & FAQs Contact Us

MCA Services
Home > MCA Services > Master Data > Company/LLP Master Data

Company/LLP Master Data

Company / LLP Name
Company/LLP/LLP/LLP/LLP

Enter Character must follow:

penger

Here a person need not be a registered user to access this particular set of information on the MCA portal. Even Guest users can access this information.

Here there is no particular need to know the CIN of the Company also, one can trace the company CIN from the search functionality above by entering its name.

The screenshot shows the MCA21 portal interface. At the top, there is a navigation bar with 'Welcome Guest', 'Forms & Downloads', 'Sitemap', 'Font Size', and 'Sign In / Sign Up'. The main header features the Ministry of Corporate Affairs logo and the tagline 'EMPOWERING BUSINESS, PROTECTING INVESTORS'. Below this, there are links for 'REGULATOR', 'INTEGRATOR', 'FACILITATOR', and 'EDUCATOR'. The search bar contains the text '*Company / LLP Name' rat'. The search results are displayed in a table with two columns: 'Company Name' and 'Company ID'.

Company Name	Company ID
RAT AND CAT DIGITAL PRIVATE LIMITED	U72900UP2017PTC094409
RAT CHINORI MARKETING LIMITED	U51909AS2011PLC010756
RAT CONTROL DEVICES (PVT) LTD	U31909DL1999PTC101481
RAT EXPORTS PRIVATE LIMITED	U15137DL2005PTC136280
RAT HOME HEALTH CARE PRIVATE LIMITED	U85190KA2023PTC161064
RAT LABS PRIVATE LIMITED	U74999GJ2021PTC123236
RAT SERVICES PRIVATE LIMITED	U74999KA2016PTC097560
RAT SOFTWARE DEVELOPERS PRIVATE LIMITED	U62099UP2023PTC179028
RAT'Z SOLUTIONS PRIVATE LIMITED	U74140DR2013PTC017507
RAT05 TECHNOLOGY LLP	AAQ-5347

Showing 1 to 10 of 476 entries

Example of the search with just three letters RAT gives us the list of the companies having RAT in their names

Selecting the company would lead us to the next screen which appears as

DSC Services

DIN Services

Master Data

- About Master Data
- View Company / LLP Master Data
- View Index of Charges
- View Signatory Details
- View Director Master Data
- View Director / Designated Partner Details
- Advanced Search

LLP Services

e-Filing

Company Services

Complaints

Document Related Services

Fee and Payment Services

Investor Services

ID Databank Registration

Track SRN/Transaction Status

Address for sending physical copy of G.A.R. 33

Public Search of Trademark

Notices Under Section 248(2)

Company/LLP Master Data

CIN	U7	809
Company Name	PRIVATE LIMITED	
RDC Code	RoC-	
Registration Number	1409	
Company Category	Company limited by Shares	
Company SubCategory	Non-govt company	
Class of Company	Private	
Authorised Capital(Rs)	100000	
Paid up Capital(Rs)	60000	
Number of Members(Applicable in case of company without Share Capital)	0	
Date of Incorporation	2	
Registered Address	027 IN	
Address other than R/o where all or any books of account and papers are maintained		
Email Id	tncat.com	
Whether Listed or not	Unlisted	
ACTIVE compliance	ACTIVE Non-Compliant	
Suspended at stock exchange	-	
Date of last AGM	-	
Date of Balance Sheet	-	
Company Status(for e-filing)	Strike Off	

Charges

Assets under charge	Charge Amount	Date of Creation	Date of Modification	Status
No Charges Exists for Company/LLP				

Directors/Signatory Details

DIN/PAN	Name	Begin date	End date	Surrendered DIN
	SINGH	24/06/17	-	
	SINGH	24/06/17	-	
	TAM	24/06/17	-	

[Export To Excel](#)
[Print](#)

- Here one person gets information as to whether the company is an active company and it is regular in filing returns.
- More importantly, one person would get to know the directors and clicking on the DIN would help in finding out the entire directorships of that particular director. This information is vital as it would help a forensic accountant detect cases of conflict of interests easily.
- One such case, a director of Company ABC was also director in PQR.
 - o The Forensic Accountant could trace this information from the MCA portal and on scrutiny of accounts of PQR, he was able to find out that this person was receiving a percentage of turnover as commission from PQR. There was substantial number of purchases for ABC happening from PQR, which turned out to be the sales of PQR. The Conflict-of-Interest angle came to light then

- Registered Users can take the documents filed in MCA portal relating to the companies on payment of a nominal fee.
 - In a Nutshell lets see what a forensic accountant gets out of such an investigation
 - Whether the Company that is investigated is active.
 - Details of Directors and their directorships to find any possible conflict of interest as a result of the same.
 - Any Director is Disqualified
 - Borrowings of the Company and Charges Created

4.2.2.2 GST Portal



- One can easily access the GST portal- there is a functionality to get the details of the Taxpayer wherein one person can take the details by just using the PAN of the person or the full GSTIN.
- The Portal Provides the Information as given below
 - Legal Name of Business
 - Trade Name
 - Effective Date of Registration
 - Constitution
 - GSTIN/UIN Status:- Says whether it is active/ inactive or it is cancelled
 - This is a vital piece of information for a forensic accountant as there are cases reported wherein forged GST papers are submitted to Bank authorities without even filing happening.
 - Other Details:- as to Administrative office, other office of the GST Department under whom the entity would operate, Nature of Business Activities and also Goods and Services dealt
 - At the end there is provision for Checking the Return Filing Frequency
 - Here also a Forensic Accountant gets vital information for decision making- as to whether the party is filing returns on time- Constant late filings are considered as red flags
 - The Picture below depicts a case of late filing-even this information helps to know whether party is originally filing returns

- o In a nutshell lets see what a forensic accountant gets out of such an investigation
 - Whether the GST bill received has the correct GST number
 - Whether GST registration number given is genuine-certain people use it to just increase their billing
 - Whether the party is regularly filing returns-or simply tax is collected and money is hoarded without paying to Government exchequer.

Search Result based on GSTIN/UIN :

Legal Name of Business	Trade Name	Effective Date of registration 06/04/2018
Constitution of Business Partnership	GSTIN / UIN Status Active	Taxpayer Type Φ Regular
Administrative Office (JURISDICTION - CENTER) Commissionerate - Division - 1 DIVISION Range -	Other Office (JURISDICTION - STATE) State Division - Circle	Principal Place of Business
Whether Aadhaar Authenticated? No	Whether e-KYC Verified? No	Additional Trade Name View

Nature Of Core Business Activity ^

Trader - Wholesaler/Distributor

Nature of Business Activities: ^

1. Retail Business 2. Wholesale Business

Dealing In Goods and Services

Goods		Services	
HSN	Description	HSN	Description
6205	MENS OR BOYS' SHIRTS		
6210	GARMENTS, MADE UP OF FABRICS OF HEADING 5602, 5603, 5903, 5906 OR 5907		
6206	WOMENS OR GIRLS BLOUSES, SHIRTS AND SHIRT-BLOUSES		
6207	MENS OR BOYS SINGLETS AND OTHER VESTS, UNDERPANTS, BRIEFS, NIGHTSHIRTS, PJAMAS, BATHROBES, DRESSING GOWNS AND SIMILAR ARTICLES ---- Underpants and brif		
6217	OTHER MADE UP CLOTHING ACCESSORIES; PARTS OF GARMENTS OR OF CLOTHING ACCESSORIES, OTHER THAN THOSE OF HEADING 6212		

HSN: Harmonized System of Nomenclature of Goods and Services

[SHOW FILING TABLE](#) [SHOW RETURN FILING FREQUENCY](#)

Filing details for GSTR3B				Filing details for GSTR-1/IFF			
Financial Year	Tax Period	Date of filing	Status	Financial Year	Tax Period	Date of filing	Status
2023-2024	June	18/07/2023	Filed	2023-2024	June	10/07/2023	Filed
2023-2024	May	16/06/2023	Filed	2023-2024	May	13/06/2023	Filed
2023-2024	April	19/05/2023	Filed	2023-2024	April	19/05/2023	Filed
2022-2023	March	17/05/2023	Filed	2022-2023	March	16/05/2023	Filed
2022-2023	February	12/05/2023	Filed	2022-2023	February	12/05/2023	Filed
2022-2023	January	11/05/2023	Filed	2022-2023	January	10/05/2023	Filed
2022-2023	December	03/05/2023	Filed	2022-2023	December	29/04/2023	Filed
2022-2023	November	25/04/2023	Filed	2022-2023	November	25/04/2023	Filed
2022-2023	October	04/01/2023	Filed	2022-2023	October	04/01/2023	Filed
2022-2023	September	02/01/2023	Filed	2022-2023	September	02/01/2023	Filed

Filing details for GSTR9			
Financial Year	Tax Period	Date of filing	Status
2021-2022	Annual	25/10/2022	Filed
2020-2021	Annual	28/12/2021	Filed
2019-2020	Annual	28/12/2021	Filed
2018-2019	Annual	29/09/2020	Filed

Image: – Show Filing Table Option from GST Portal

The information that is derived from GST portal is available even to a guest user, that is the Forensic Accountant need not be a person who has taken GST registration, instead can browse this information easily as a guest user.

Other Techniques Include

Ratio Analysis

- Analysing the Financial Statements of the company using techniques such as Ratio Analysis would help in identifying possible instances of fraud or manipulations in accounts

Illustration

Given below are the extracts from a company’s Financial Statements – which deals in Retail Trade of Jewels.

Let us compute the Debtors to Sales Ratio for the company for the two years

Particulars (Amount in Crores Rupees)	2016-17	2015-16
Trade Receivables	8,567.01	6910.14
Revenue from Operations	10,464.76	10750.72
Receivables to Sales	81.87	64.28

Particulars	Note No.	March 31, 2017	March 31, 2016
ASSETS			
Non-Current Assets			
Property, Plant and Equipment	3	25,827.54	27,289.02
Capital Work-In-Progress		-	-
Financial Assets			
i) Investments	4	101,361.05	102,347.14
ii) Loans	5	1,235.50	1,596.47
iii) Other Non Current Financial Assets	6	2,885.23	4,043.07
Deferred Tax Assets [Net]		5,633.00	4,257.97
Other Non-Current Assets	7	859.14	865.79
		<u>137,801.46</u>	<u>140,399.46</u>
Current Assets			
Inventories	8	253,055.40	183,566.07
Financial Assets			
i) Trade Receivables	9	<u>856,701.75</u>	<u>691,014.82</u>
ii) Cash and Cash Equivalents	10	6,221.06	3,710.42
iii) Other Bank Balances	11	11,326.52	9,718.38
iv) Loans	12	23,140.67	28,690.47
v) Other Current Financial Assets	13	2,796.45	850.47
Current Tax Assets [Net]	14	3,277.12	1,770.29
Other Current Assets	15	8,255.40	18,713.61
		<u>1,164,774.37</u>	<u>938,034.53</u>

STATEMENT OF PROFIT & LOSS FOR THE YEAR ENDED,			
Particulars	Note No.	(₹ in Lacs)	
		March 31,2017	March 31,2016
REVENUE			
Revenue From Operations	27	<u>1,046,476.60</u>	<u>1,075,072.31</u>
Other Income	28	14,650.33	6,486.99
Total Revenue		<u>1,061,126.93</u>	<u>1,081,559.30</u>

The Calculation Gives a percentage of 81.87 % meaning either 81.87% of the Customers are buying jewels and leaving without paying cash or they are purchasing on credit.

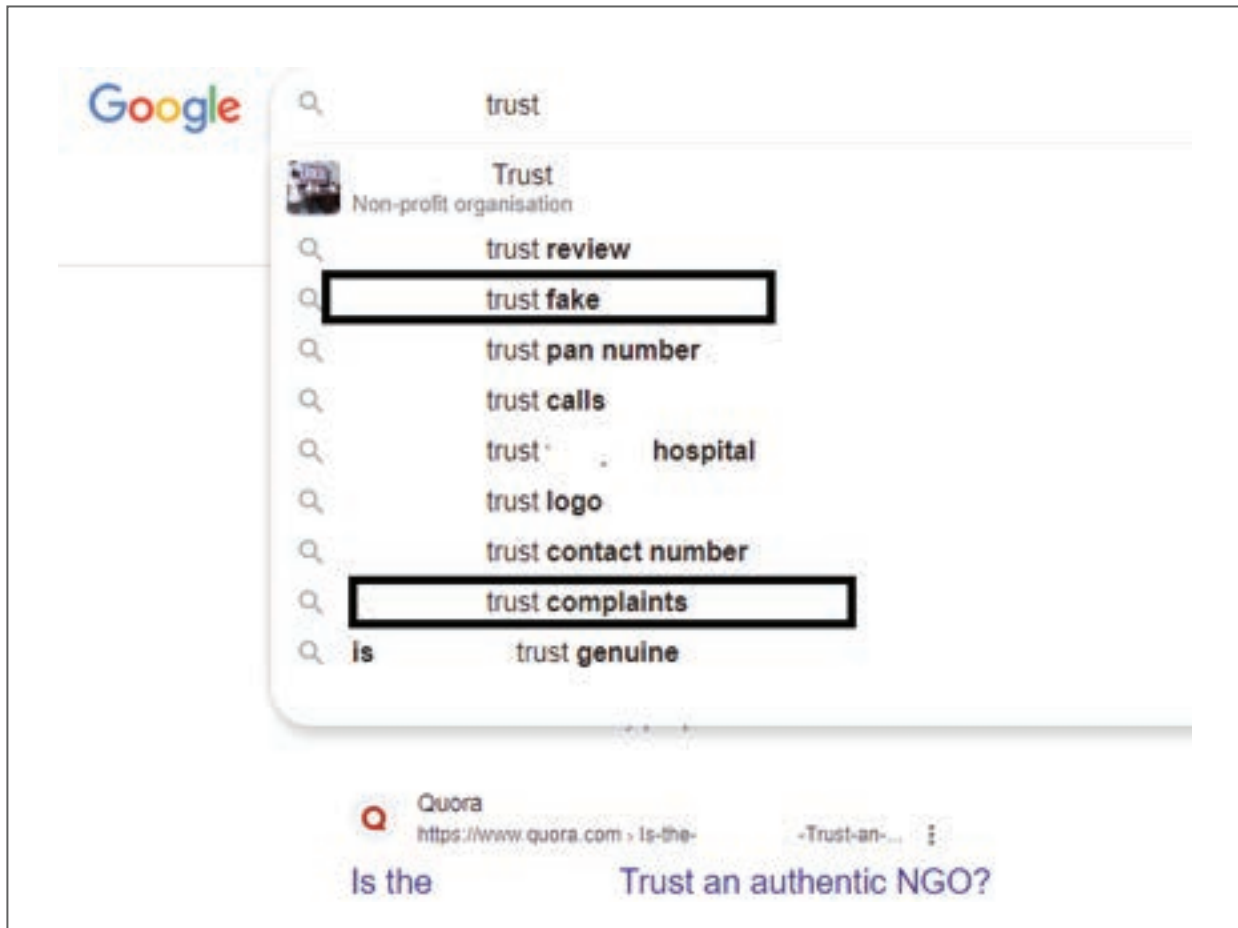
There is another probability of longer credit periods given to customers -which is again not practiced in this form of business anywhere.

Probably, the entity would have resorted to manipulations in accounts by showing fictitious sales and adjusting the same in receivables.

These kinds of frauds could be easily traced by knowing the client's nature of business and doing a comparison with what is shown in the accounts.

Google

- The Picture that is depicted below suggests how google can help a forensic accountant
- Just by entering the Name of the organisation-Google provides as many details
- When the name is entered Google Provides us with the searches done earlier and sometimes it throws light on many aspects, the forensic accountant is unaware of
- Even without this dropdown coming, Forensic Accountant can directly type in words like “Dispute, Case, Fraud” along with the name of the Company and Google would provide the data which supports that search



In the image above, it was a search to find out the genuineness of an NGO before the Company was about to do a CSR spending.

Typing the name of the trust brought key words in dropdown like “Fake, Complaints”, etc.

The forensic accountant continued the process by selecting the keywords and continued the search and finally the same brought to light many things which were not found before

Zauba Corp

- This website provides commercial information and insights on businesses and helping the prospective stakeholders like creditors take a call before deciding on alliances, coalition etc.



Zauba Corp helps you know financial performance of businesses you deal with

Access critical documents and information for facts based decision making

4.2.3 SOME FRAUDULENT ACTIVITIES CARRIED OUT BY ORGANISATIONS

Creation of Ghost Employees

An organisation may resort to the creation of Ghost Employees. an employee who does not exist
Three possible cases

- A deceased employee
- Employee who has resigned from the organisation but still continues in books
- A Person who is not at all there in the organisation

Here, the third category is the one wherein the organisation creates a profile for a person who is not at all employed in the entity but is recorded as receiving emoluments from the company

Some organisations practice this.
Let's see the modus operandi



- Organisation invites applications for a particular post, say clerk –say 10 vacancies
- They receive application from 100 prospective people who are called for the interview
- These 100 people are supposed to come for the interview with copies of their certificates and also the ID proofs
- During the interview, the organisation collects a copy of the certificates and ID proofs and the applicants are informed that the results would be published later
- Later on 10 people are selected and the remaining rejected ones, their IDs remain with the employer
- Employer uses the credentials so received for creating the so called “Ghost Employees”
- The Profile is created and the salary is paid through cash.

In these cases, scrutiny of the PF records would help the Forensic Accountant find the true facts of the case.

Fake Land Documents

There are cases when fake documents are submitted by the party claiming ownership of immovable property

A Forensic Accountant can check whether the same is genuine through

- Checking the same with the Land records
- Even by checking the property Tax payment portals the owner details could be fetched and found out.



Vehicle Related Frauds

Vehicle related frauds can be found out by verifying the Registration Certificate along with a tour of the Vahan Portal as the same provides details of the Registered Vehicle, Owner details, etc



VAHAN
NR e-Services

Ministry of Road Transport & Highways
Government of India

Home Parivahan Know Your Vehicle Details Contact us

MULTIPLE CHOICE QUESTIONS (MCQ) FOR PRACTICE

- 1 To get the Company Master Information from the MCA portal (Choose the most appropriate answer)
 - a) One need to be a registered user in the Portal
 - b) One need not be a registered user in the Portal
 - c) One need to have a valid DIN
 - d) One need to be a professional of ICAI, ICSI or ICMAI.

- 2 To access details of a registered person under GST in GST Portal, (Choose the Most Appropriate Answer)
 - a) GSTIN is mandatory
 - b) PAN is sufficient
 - c) GSTIN along with OTP to the registered person's Mobile number is needed
 - d) GST Portal user ID and password of the registered person is needed.

**DESCRIPTIVE QUESTIONS**

- 1 Explain Ghost Employees as Mechanism to do fraud

- 2 Explain how the Related party Transactions can be traced through MCA portal.

CHAPTER 5

FRAUD PREVENTION AND DETERRENCE



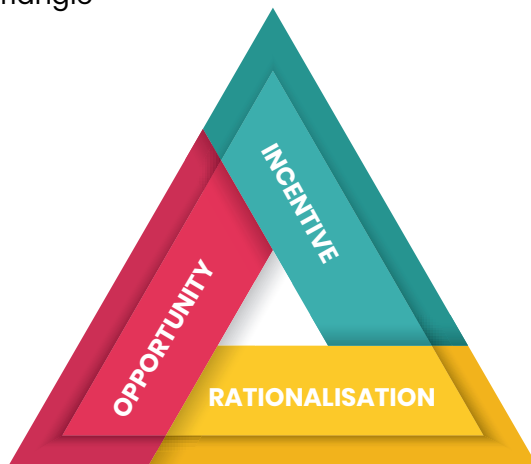
LEARNING OBJECTIVES

- Fraud Prevention
- Fraud Triangle
- Fraud Diamond

5.1 FRAUD PREVENTION

Fraud prevention mechanisms should exist within the organisations to ensure that the circumstances paving way for the fraud occurrence are kept to the minimum

Before discussing about the Fraud prevention Mechanism, Lets look into the concept of Fraud Triangle



- This concept lays down the factors which should be present for the fraud to happen
- This concept even says, that existence of all the factors mentioned are necessary for the fraud to happen, that is, if any of the factor is missing, then fraud will not happen, despite all other factors being present
- The Factors are
 - Opportunity
 - Incentive
 - Rationalisation

- Opportunity refers to the conducive conditions to do fraud
- Incentive refers to the driving factors that instigate a person to do fraud
- Rationalisation is what makes one feel that what he/she is doing is right

Lets take few examples to understand this concept better`

Case 1:- A Person trying a pickpocket

Opportunity	<ul style="list-style-type: none"> • The Person trying to carry out pickpocket is now at a Railway Station • There is huge rush • There is a gentleman who is busy on phone with wallet in his pocket just hanging out and he is unaware of things happening around him • Surrounding the gentleman is a big crowd waiting for the train and no one is noticing him • There are no CCTV cameras in near vicinity.
-------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Incentive	<ul style="list-style-type: none"> • The Close relative of the fraudster is at hospital and he is in urgent need of money • The person needs the funds to be arranged very fast and his normal salary will not be sufficient • Tried collecting funds from different sources but that will not be sufficient for the occasion
Rationalisation	<ul style="list-style-type: none"> • The person feels that the target or the person on phone is a rich person and this theft will not cause substantial harm for him • The Fraudster feels what he is doing is right considering the circumstances

Here, all the three must exist for the fraud to happen

- Say there is a person attempting pickpocket at railway station but there is no such person who is busy on phone and also there is no crowd-despite the fact that there is pressure on the fraudster to do fraud and also, he feels what he is doing is right, he will not carry this out.
- The next case is when the Opportunity and Incentive exist but there exist a feeling in the minds of the person that what he/she is doing is not right so the fraud will not materialize
- The third case is when the Opportunity is present and so is Rationalisation but there is no particular need or financial pressures on the part of the person to do fraud, the person is a salaried employee with a fixed monthly salary which is sufficient to meet all needs-here also fraud will not happen.

Case 2 :- Meeting Investor Expectations

Here it's the case of a Listed Company
The story goes on these lines

- The listed Company is supposed to publish the results on quarterly basis, i.e., April to June, July to September, October to December, January to March
- The Company is supposed to give a prior intimation before the results are published
- In the given case, our company had given the statement that the Quarterly Results for April to June quarter shall be published on 26th July, 2023 and the announcement was made on 04th July,2023
- Once the above announcement happens, Analysts will take charge, Analysts are the people who normally predict the Financial Results well in advance and publish the same in the form of a research report.
- During this tenure, 4th July and 26th July, that is when the announcement is made and when the results would be published, Analysts would come up with the forecast

Name	Date of Forecast Report	Expected Growth in Profits of the Company as per report
Analyst -1	07-07-2023	12%
Analyst -2	11-07-2023	17%
Analyst -3	17-07-2023	14%
Analyst-4	21-07-2023	16%

- Industry as a result of this Forecast would expect profit growth in the range of 12-17% and Stock prices would have also moved accordingly.
- Say, there is an audit committee/directors meeting happening on 22nd July to discuss the draft numbers and they find that the actual growth in Profits is only a meagre one, only 4%
- The Directors would analyse the situation as to what is to be done- real result if published will lead to drastic fall in share prices and there will be question on worth and credibility of the company.
- Therefore they would possibly consider manipulating the numbers to ensure it meets the investor and analyst expectations
- Finally, what is announced on 26th July is manipulated results.

Here, the Top Management feels that what they have done is something which is practiced by the other entities,i.e. it is a common practice and therefore there is no wrong whatsoever.

These are the common examples for the Fraud Triangle

However there is an additional dimension added -which is capability in Fraud Diamond Concept

Capability Factor refers to

- The right organizational position to commit a fraud
- Expertise to do the same
- Ability to cope up with the stress associated with the fraud
- Being a good liar

In the above Case No 2 relating to the manipulation of numbers by Management to meet the investor and analyst expectations, the people doing the fraud must be at the Top Level, occupying the hot seat in the organisation, a person who is occupying the lower level in an organisation or who is a supervisor will not be able to do the same

To do the fraud in Case 2, The persons should have the adequate expertise to do the same. Top Management should know the ways to execute the same in the most effective manner.

Doing a fraudulent activity, would make a person have sleepless nights, with the fear of getting caught at any time, so the person should be able to deal with the so-called stress

A person should have the skills to tell lies and to cover up one lie thousand lies need to be again said, the person should be capable of doing all this

5.2 FRAUD PREVENTION AND DETERRENCE MEASURES

- Proper tone at the top:- Management can lay down Policies and procedures for the proper functioning of the Internal Control Mechanisms within the business
- Continuous Monitoring and evaluation:-Management can ensure that the fraud cases are kept to the minimum by continuously monitoring its plans and also controls
- Introduction of Internal Audit Mechanism:- To ensure that there is continuous monitoring from a third eye perspective, an effective internal audit mechanism would be of great use
- Thorough Check on the employees:-Organisation should ensure there is thorough check on the employees to find their present living standards and also their whereabouts
- Segregation of Duties:- Segregation of Duties among the staff and also rotation of staff at reasonable intervals would also help in keeping a check on the fraud



5.3 CONCLUSION

- Frauds have grown over the years and would continue to grow
- Controls would be discovered but fraudsters would still find ways to override them
- The saying goes" Prevention is better than cure" and organisations should strive towards ensuring that they have pro active strategies to prevent frauds from occurring rather than being Re-active which is taking action after the frauds have occurred.

MULTIPLE CHOICE QUESTIONS (MCQ) FOR PRACTICE

- 1 The Additional factor included in Fraud Diamond apart from the ones which are there in Fraud Triangle is
 - a) Opportunity
 - b) Incentive
 - c) Rationalisation
 - d) Capability

- 2 Segregation of Duties would prevent which one of the dimensions within fraud diamond to happen
 - a) Opportunity
 - b) Incentive
 - c) Rationalisation
 - d) Capability

- 3 Rationalisation in Fraud Triangle refers to
 - a) The inner urge within a person that what that person is doing is right
 - b) The factors leading the person to commit a fraud
 - c) Weak internal controls within the organisation promoting a fraud
 - d) Poor tone at the top leading to a fraud

DESCRIPTIVE QUESTIONS

- 1 Explain the "Incentive" in Fraud Triangle
- 2 Briefly Explain the Capability aspect in Fraud Diamond
- 3 Explain a few fraud deterrence and prevention measures

UNIT

2

Basics of
Digital Forensic and
Cyber Security

CHAPTER 1

INTRODUCTION TO CYBERCRIME



LEARNING OBJECTIVES

- Understanding the fundamentals of Cybercrime
- Understanding Cyber Security
- Different types of cyber crimes
- Reasons for cyber crimes
- Types of cyber attacks

1.1 INTRODUCTION TO CYBERCRIME

Cybercrime may be defined as “Any attack on the information systems or any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime”.

The attack can be on the confidentiality of information, on the integrity of information, or it can be a denial-of-service attack or a repudiation attack. The attack can be on an individual, an enterprise or on a government.

Here are some examples of cyber-crime: Intentionally sending a virus is a crime. Stealing credit card information during an e-commerce transaction, impersonating a student in an e-learning portal, an employee sending confidential information of an organization to an outsider through email etc., are cyber-crimes. However, the definition of what a crime is differs from country to country. In some countries, it is not a crime to visit adult sites, but in some countries, it is a crime, the punishment can be imprisonment. In some countries, it is OK to visit adult sites, but the downloaded content cannot be sent to another person.

Consider this case: a person created a mail account with a free mail service provider and then he sent a threatening mail to a person. Again, the person received another threatening mail, but now from a different mail address, but with the same email service provider. Perhaps this criminal was creating mail accounts and was using it only once. The email service provider is based in the US and the person is in India. Think of it, how do you catch the criminal?

In India, Cyber Crimes are mainly relative to what the Information Technology Act-2000/ 2008 has defined.

1.2 CYBER-ATTACK

Cyber-attack is any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system.

These can be labelled as either a Cyber campaign, cyber warfare or cyber terrorism in different context. Cyber-attacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nations. Cyber-attacks have become increasingly sophisticated and dangerous.

1.3 CYBER WARFARE AND CYBER TERRORISM

Cyber warfare utilizes techniques of defending and attacking information and computer networks that inhabit cyberspace, often through a prolonged Cyber campaign or series of related campaigns. It denies an opponent 's ability to do the same, while employing technological instruments of war to attack an opponent 's critical computer systems. Cyber terrorism, on the other hand, is the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population. That means the end result of both cyber warfare and cyber terrorism is the same, to damage critical infrastructures and computer systems linked together within the confines of cyberspace. There were two such instances between India and Pakistan that involved cyberspace conflicts, started in 1990s. Earlier cyber-attacks came to known as early as in 1999. Since then, India and Pakistan were engaged in a long-term dispute over Kashmir which moved into cyberspace. Historical accounts indicated that each country's hackers have been repeatedly involved in attacking each other's computing database system. The number of attacks has grown yearly.

1.4 WHAT IS CYBER SECURITY?

Cyber Security, also referred as Network Security or Computer Security or IT Security, is the body of technologies, processes, and practices designed to protect networks, computers, and data from attacks, thefts, damages, and unauthorized accesses. Cyber security can be defined as the "preservation of confidentiality, integrity and availability of information in the cyberspace.



1.5 WHY CYBER SECURITY IS CRITICAL

- All our assets and our lives are virtualized and have gradually moved to Cyber world. Where there are assets, definitely there is greater temptation to steal assets.
- Everything is connected and everyone is connected.
- So many components between sources to destination including switches, routers, protocols, software, ISPs are involved to carry the information.
- Software applications can interact with each other without user intervention.
- Trillions of dollars of online business happen every year.

1.6 DIFFERENT TYPES OF CYBER CRIMES

The various broad types of Cyber Crimes that we should be familiar with are

- 1 Unauthorized Access to a Computer (on the Internet or on a private network)
- 2 Causing Damage to the property of another person using a computer.
- 3 Fraudulent use of the property belonging to others using a computer.
- 4 Violation of Privacy using a computer

Under the generic description of crimes mentioned above, we can specify the following specific cybercrimes.

- **Spamming**
Spamming is the use of messaging systems to send multiple unsolicited messages (spam) to large numbers of recipients for the purpose of commercial advertising, for any prohibited purpose (especially the fraudulent purpose of phishing), or simply repeatedly sending the same message to the same user. While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media: instant messaging spam, Web search engine spam, spam in blogs, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social spam, spam mobile apps and file sharing spam. A person who creates spam is called a spammer.
- **Phishing**
Phishing is a type of fraud / attack where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message or email designed to trick the recipient into revealing sensitive information to the attacker or downloading malware by clicking on a hyperlink in the message that appear to be from a legitimate source. Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim. As of 2020, phishing is by far the most common attack performed by cybercriminal.
- **Cyber Bullying**
Cyberbullying or cyber harassment is a form of bullying or harassment using electronic or communication devices such as computer, mobile phone, laptop, etc. It has become increasingly common, especially among teenagers, as the digital sphere has expanded,

and technology has advanced. Cyberbullying is when someone, typically a teenager, bullies or harasses others on the internet and other digital spaces, particularly on social media sites. Harmful bullying behavior can include posting rumors, threats, sexual remarks, a victims' personal information, or pejorative labels (i.e. hate speech). Bullying or harassment can be identified by repeated behavior and an intent to harm.

- **Cyber Stalking**

Cyber stalking is the use of electronic communication by a person to follow a person, or attempts to contact a person to foster personal interaction repeatedly despite a clear indication of disinterest by such person. It may include false accusations, defamation and slander. It may also include monitoring, identity theft, threats and blackmail.

- **Cyber Warfare**

Cyber warfare involves nation-states using information technology to penetrate another nation's networks to cause damage or disruption. Cyber warfare has been acknowledged as the fifth domain of warfare (following land, sea, air, and space). A cyber warfare attack may intrude networks for the purpose of compromising valuable data, degrading communications, impairing infrastructural services such as transportation and medical services, or interrupting commerce. Cyber terrorism is also the disruptive use of information technology by terrorist groups to further their ideological or political agenda.

- **Cyber-squatting**

Cyber-Squatting is an act of registering, trafficking in, or using a domain name with intent to profit from the goodwill of a trademark belonging to someone else.

- **Espionage**

Espionage is the act or practice of obtaining data and information without the permission and knowledge of the owner.

- **Child Pornography**

Child Pornography / Child sexually abusive material (CSAM) refers to material containing sexual image in any form, of a child who is abused or sexually exploited. It is punishable for Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form.

- **Cyber Grooming**

When a person builds an online relationship with a young person and tricks or pressures him/her into doing sexual act, it is Cyber grooming.

- **Vishing**

Vishing is an attempt where fraudsters try to seek personal information like Customer ID, Net Banking password, ATMPIN, OTP, Card expiry date, CVV etc. through a phone call.

- **SMS Phishing**

It is the fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers. It is also called Smishing.

- **Impersonation and Identity theft**

Impersonation and identity theft is an act of fraudulently or dishonestly making use of the electronic signature, password or any other unique identification feature of any other person.

- **Ransomware**

An attack that involves encrypting data on the target system holding data as a hostage and demanding a ransom in exchange for letting the user have access to the data again by decrypting it after paying ransom.

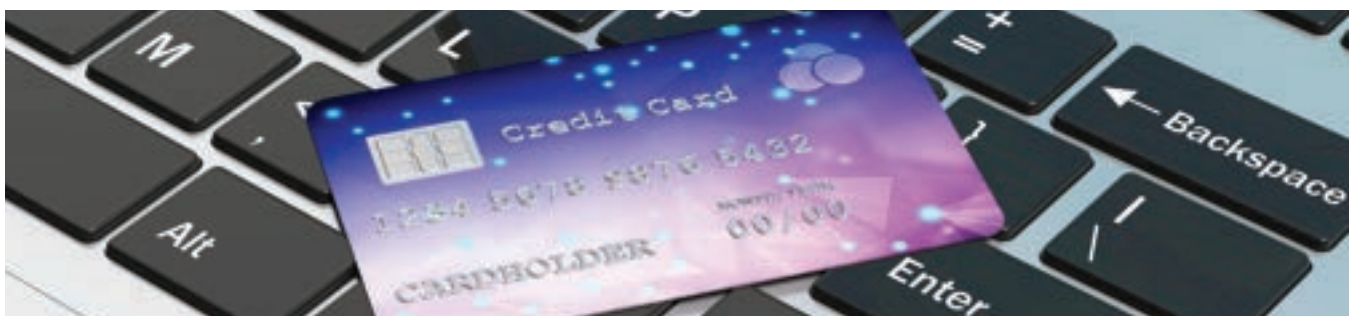
- **Advanced Persistent Threats (APTs):**

This refers to an attack that focuses on stealing information from the victim machine without its user being aware of it. These attacks are generally targeted at large companies and government networks. Because APT attacks are slow in nature, their effect on computer performance and Internet connections is negligible. APTs exploit vulnerabilities in the applications running on computers, operating systems, and embedded systems.

1.7 REASONS FOR COMMISSION OF CYBER CRIMES

There are many reasons, which act as a catalyst in the growth of cybercrime. Some of the prominent reasons are:

- Money: People are motivated towards committing cybercrime for making quick and easy money.
- Revenge: Some people try to take revenge on other people/organization/society/ caste or religion by defaming its reputation or bringing economical or physical loss. This comes under the category of cyber terrorism.
- Fun: amateurs do cybercrime for fun. They just want to test the latest tool they have encountered.
- Recognition: It is considered to be prided if someone hack the highly secured networks like defense sites or networks.
- Anonymity: Many time the anonymity that a cyber space provide motivates the person to commit cybercrime as it is much easy to commit a cybercrime over the cyber space and remain anonymous as compared to real world. It is much easier to get away with criminal activity in a cyber-world than in the real world. There is a strong sense of anonymity than can draw otherwise respectable citizens to abandon their ethics in pursuit personal gain.
- Cyber Espionage: At times, the government itself is involved in cyber trespassing to keep eye on other person/network/country. The reason could be politically, economically or socially motivated.



1.8 TYPES OF ATTACKERS

The various broad types of Cyber Crimes that we should be familiar with are

- **Hacker**
Hacker is a general term that has historically been used to describe a computer-programming expert. More recently, this term is commonly used in a negative way to describe an individual who attempts to gain unauthorized access to network resources with malicious intent.
- **Cracker**
Cracker is the term that is generally regarded as the more accurate word that is used to describe an individual who attempts to gain unauthorized access to network resources with malicious intent.
- **Phreaker**
A phreaker is an individual who manipulates the phone network to cause it to perform a function that is normally not allowed. A common goal of phreaking is breaking into the phone network, usually through a pay phone, to make free long-distance calls.
- **Spammer**
A spammer is an individual who sends large numbers of unsolicited e-mail messages. Spammers often use viruses to take control of home computers and use those computers to send out their bulk messages.
- **Phisher**
A phisher uses e-mail or other means in an attempt to trick others into providing sensitive information, such as credit card numbers or passwords. The phisher masquerades as a trusted party that would have a legitimate need for sensitive information.
- **White hat**
White hat is a term used to describe individuals who use their abilities to find vulnerabilities in systems or networks and then report these vulnerabilities to the owners of the system so that they can be fixed.
- **Black hat**
Black hat is another term for individuals who use their knowledge of computer systems to break in to systems or networks with the malicious intention that they are not authorized to use.

1.9 Different types of Cyber Attacks

The threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices. Typically, the network devices under attack are the end points, such as servers and desktops. There are four primary classes of attacks exist:

- **Reconnaissance**
- **Access**
- **Denial of service**
- **Viruses, Worms, and Trojan horses (Malwares)**

- **RECONNAISSANCE**

Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities. It is also known as information gathering and, in most cases, it precedes an actual access or denial-of-service attack. Reconnaissance is somewhat analogous to a thief casing a neighborhood for vulnerable homes to break into, such as an unoccupied residence, easy-to-open doors, or open windows. Reconnaissance attacks can consist of the following:

- o Packet sniffers
- o Port scans
- o Ping sweeps
- o Internet information queries

- **ACCESS**

System access is the ability for an unauthorized intruder to gain access to a device for which the intruder does not have an account or a password. Access attacks exploit known vulnerabilities in authentication services, ftp services, and web services to gain entry to web accounts, confidential databases, and other sensitive information. Access attacks can consist of the following:

- o Password attacks
- o Trust exploitation
- o Port redirection
- o Man-in-the-middle attacks

- **Password Attacks**

Password attacks can be implemented using several methods, including brute-force attacks, Trojan horse programs, IP spoofing, and packet sniffers. Although packet sniffers and IP spoofing can yield user accounts and passwords, password attacks usually refer to repeated attempts to identify a user account, password, or both. These repeated attempts are called brute-force attacks.



- **Trust Exploitation**

Although it is more of a technique than a hack itself, trust exploitation refers to an attack in which an individual takes advantage of a trust relationship within a network. When all servers or systems reside on the same segment, compromise of one system can lead to the compromise of other systems because these systems usually trust each other attached to the same network (System-A trusts System-B, System-B trusts everyone, System-A trusts everyone). Another example is a system on the outside of a firewall that has a trust relationship with a system on the inside of a firewall. If that trusted outside system is compromised, it can take advantage of that trust relationship to attack the inside network.

- **Port Redirection**

Port redirection attacks are a type of trust exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped. Consider a firewall with three interfaces and a host on each interface. The host on the outside can reach the host on the public services segment, but not the host on the inside. This publicly accessible segment is commonly referred to as a demilitarized zone (DMZ). The host on the public services segment can reach the host on both the outside and the inside. If hackers were able to compromise the public services segment host, they could install software to redirect traffic from the outside host directly to the inside host. Although neither communication violates the rules implemented in the firewall, the outside host has now achieved connectivity to the inside host through the port redirection process on the public services host. An example of an application that can provide this type of access is Net cat. Proper trust models and host-based IDS can detect a hacker and prevent installation of such utilities on a host.

- **Man-in-the-Middle attack (packet sniffer)**

A packet sniffer is a device or program that allows eavesdropping on traffic travelling between networked computers. The packet sniffer will capture data that is addressed to other machines, saving it for later analysis. An example could be someone who is working for an Internet service provider (ISP) and has access to all network packets transferred between the ISP network and any other network. Man in the middle attack where a middleman impersonates each end point and is thus able to manipulate both victims. The sender and recipient believe they are communicating directly with one another. By using strong encryption like IPsec tunnels makes packet sniffing useless which would allow the hacker to see only cipher text.

- **DENIAL OF SERVICE (DOS)**

Denial of service implies that an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users. DoS attacks involve either crashing the system or slowing it down to the point that it is unusable. In most cases, performing the attack simply involves running a hack or script. DoS attacks are the most feared one because attacker does not need prior access to the target.

- **Distributed Denial-of-Service Attacks**

They are designed to saturate network links with spurious data. This data can overwhelm an Internet link, causing legitimate traffic to be dropped. DoS uses attack methods similar to standard DoS attacks but operate on a much larger scale. Typically, hundreds or thousands of attack points attempt to overwhelm the target.

- **MALWARE (VIRUSES, WORMS, TROJANS ETC.)**

Cyber criminals operate remotely, in what is called 'automation at a distance' using numerous means of attacks available, which broadly fall under the umbrella term of malware (malicious software). All malicious software are intended to be inserted into the network with the intention of making some loss or the other. Some of the malwares and their behavior are given below:

- **Viruses**

Computer Virus is a program written to enter to your computer and damage/ alter your files/data and replicate themselves and spread from one computer to another by attaching itself to another computer file.

- **Worms**

Worms are self-replicating and do not require a program to attach themselves to. Worms continually look for vulnerabilities and report to the worm author when weaknesses are discovered.

- **Trojan horses**

Trojans open a back door entry to your computer, which gives malicious users/ programs access to your system, allowing confidential and personal information to be theft. A software program appears to perform one function (for example, virus removal) but actually acts as something else. For example, an attacker might log into a Windows box and run a program that looks like the true Windows log on screen, prompting a user to type his username and password.

- **Spyware**

By opening attachments, clicking links or downloading infected software, from infected e-mails spyware is installed on your computer. Spyware can enter your computer systems and can secretly monitor what employee type and record account numbers and passwords without your knowledge.

- **Adware**

Adware installs itself in a similar manner to spyware, though it typically just displays extra advertisements when you are online. Adware can slow down your computer and it can be frustrating to try to close all the extra pop-up windows, but it will not destroy your data.

- **Spam ware**

SPAM is “flooding the Internet with many copies of the same message. SPAM may not be the biggest risk but screening and deleting junk e-mail wastes our time and if a junk e-mail attachment is opened, it may release a virus. SPAM filters are an effective way to stop SPAM; these filters come with most of the e-mail providers online. Also, you can buy a variety of SPAM filters that work effectively.

- **Botnet**

A Compromised device in a computer network is known as a bot. (short of ‘robot’ also known as a zombie).A botnet is a collection of internet-connected computers whose security defenses have been breached and control ceded to a malicious party and have been set up to forward transmissions (including spam or viruses) to other computers on the internet without knowing their owners (acting as a hub that forwards malicious files etc. to other computers). Criminals use botnets to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud. If your computer becomes part of a botnet, your computer might slow down and you might inadvertently be helping criminals



SUMMARY

In summary, cybercrime is a broad category encompassing unlawful activities involving computers, communication devices, and networks. It can range from stealing sensitive information to disrupting critical infrastructures. The definition and consequences of cybercrimes vary across countries. Cybersecurity is crucial in this digital age due to the virtualization of assets, interconnectedness, and the significant financial stakes involved in online businesses. Various types of cybercrimes exist, including unauthorized access, property damage, fraudulent property use, and privacy violations, with specific examples like spamming, phishing, and cyberbullying falling under these categories. Motivations for committing cybercrimes range from financial gain and revenge to personal amusement and even state-sponsored espionage.

CHAPTER 2

RECENT TRENDS IN CYBERCRIME

CYBER FRAUDS IN FINANCIAL SECTORS



LEARNING OBJECTIVES

- ✓ To understand cyber crimes
- ✓ To explore recent trends in cybercrime
- ✓ To gain knowledge about cyber frauds in financial sectors
- ✓ How to prevent cybercrimes in financial sectors

2.1 INTRODUCTION

The recent advancements in technology have made mankind dependent on the Internet to a large extent. Internet has found a place in our everyday lives in terms of communication, online shopping, storing data, online reservation, game in, Finance sector etc. However, this over dependency on the Internet has given rise to a number of cybercrimes. Cybercrimes is a general term wherein the computer is either a tool or a target or a medium of communication for carrying out criminal activity. It also covers the traditional crimes in which computers or networks are used to enable the illicit activity.



Digital financial services (DFS) hold great promise as a means to enable financial inclusion and thus help improve people's lives. However, cybercrime has become a key concern in developing and emerging countries' financial markets and is threatening to hinder global advances in building more inclusive financial sectors.

Over recent years, financial markets in Sub-Saharan Africa, the East Asia and Pacific region, Latin America and South Asia have been affected by a rapid increase in the number of cyber incidents and data breaches and particularly affected are those markets with higher volumes of DFS transactions.

While markets in Asia are recording the highest use rates of mobile banking and digital payment applications, they are also experiencing the highest volume of cyberattacks on financial institutions.

Falling victim to a scam or experiencing system access errors can result in financial and psychological harm and will most certainly affect a customer's confidence and trust in the financial service.

Following are the points that leads to financial loss and customer dissatisfaction over the Digital Financial Services:

- Significant cause of customer dissatisfaction with DFS provider services is unplanned system outages.
- Research on the attitudes and behaviors of low-income mobile money users shows that inability to transact due to network or service downtime was rated as one of the greatest annoyances and resulted in irresponsible behaviors that put the users at risk of being defrauded.
- The negative experiences prove to determine DFS consumers from using mobile money services more frequently and significantly decreased the level of trust in providers and the financial system altogether.
- At least 5 people are particularly vulnerable to fraud and system access errors that can result from a cyber incident.
Consumers are often less aware and educated about social engineering attacks.
- Consumers are more likely to use devices and channels that are not designed to offer the security needed for a financial transaction (e.g., USSD technology) and, most importantly, they cannot afford to lose money.

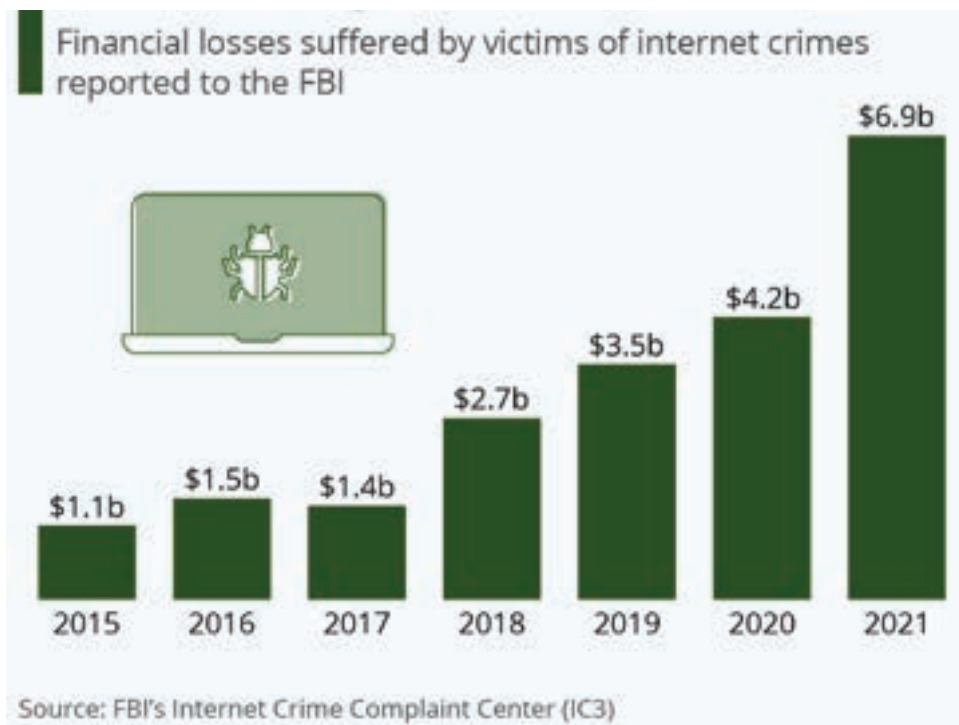
Another problem is that in developing countries customers are often liable for losses associated with a cyber incident, or they bear the burden of proving that they were the victim.

- In 2016 the International Telecommunication Union (ITU) and CGAP surveyed 5,220 mobile money users from Ghana, the Philippines and Tanzania. Fraudulent or scam SMSs had been received by 83% of the Philippine respondents, 56% of the Ghanaian respondents and 27% of the Tanzanian respondents.
- In both the Philippines and Tanzania, 17% of the mobile money users interviewed reported having lost money to a fraud or a scam, while 12% of the Ghanaian respondents made the same admission.
- Because trust and confidence in financial service providers (FSPs) and payment systems are key ingredients for sustained financial inclusion, cyber incidents and their associated losses can hinder efforts to expand access to financial services.

Furthermore, these kinds of incidents and customers' negative

International convening and standard-setting bodies like the G7, the G20 Finance Ministers and Central Bank Governors, and the Committee on Payments and Market Infrastructures (CPMI) at the Bank for International Settlements (BIS) have recognized the risk of cybercrime in the financial sector and the need for a global response to it.

As a result of this increased attention, cyber risk is now largely acknowledged as "a growing and significant threat to the integrity, efficiency and soundness of financial markets worldwide



2.2 RECENT TRENDING IN CYBERCRIME ATTACK

➤ **Ransomware Attacks:**

Ransomware can be traced back to 1989 when the “AIDS virus” was used to extort funds from ransomware recipients. Payments for that attack were mailed to Panama, at which point a decryption key was sent back to the user.

In 1996, Columbia University’s Moti Yung and Adam Young introduced ransomware known as “crypto viral extortion.” This idea, born in academia, illustrated the progression, strength, and creation of modern cryptographic tools.

Young and Yung presented the first crypto virology attack at the 1996 IEEE Security and Privacy Conference. Their virus contained the attacker’s public key and encrypted the victim’s files.

The malware then prompted the victim to send asymmetric ciphertext to the attacker to decipher and return the decryption key—for a fee.

Attackers have grown creative over the years by requiring payments that are nearly impossible to trace, which helps cybercriminals remain anonymous. For example, the notorious mobile ransomware Fusob requires victims to pay using Apple iTunes gift cards instead of standard currencies, like dollars.

Ransomware attacks began to soar in popularity with the growth of cryptocurrencies, such as Bitcoin. Cryptocurrency is a digital currency that uses encryption techniques to verify and secure transactions and control the creation of new units. Beyond Bitcoin, there are other popular cryptocurrencies that attackers prompt victims to use, such as Ethereum, Litecoin, and Ripple.

Ransomware has attacked organizations in nearly every vertical, with one of the most famous viruses being the attacks on Presbyterian Memorial Hospital. This attack infected labs, pharmacies and emergency rooms, highlighting the potential damage and risks of ransomware.

➤ **Supply Chain Attacks:**

A supply chain attack is a type of cyber-attack that targets organizations by focusing on weaker links in an organization’s supply chain.

The supply chain is the network of all the individuals, organizations, resources, activities and technology involved in the creation and sale of a product.

The goal of a supply chain attack is to infiltrate and disrupt a weak point of a system within an organization’s supply chain with the intent to cause harm.

One typical way of doing this is by attacking a third-party supplier or vendor connected to the actual target. Attacks are typically made on third parties that are considered to have the weakest cybersecurity measures by the attacker.

When the weakest point in the supply chain is identified, the hackers can focus on attacking the main target with the supply chain attack.

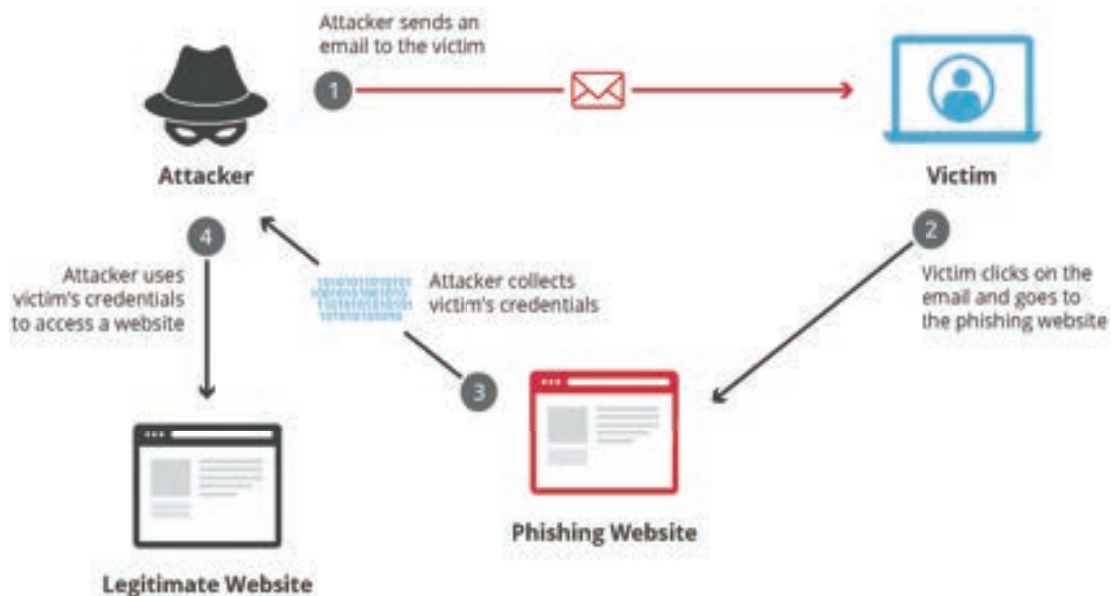


To effectively detect supply chain attacks, an organization should first have a systematic verification process in place for all the possible pathways into a system. An inventory of all the assets and data pathways within a supply chain should be made, which should help in detecting potential security gaps within a system. The next step would be to create a threat model of the organization's environment. The threat models can include assigning assets to adversary categories. The categories can then be rated, which will help in determining how severe a threat of an attack could be. These scores should be continually updated. Assets should be classified by most at risk to least at risk.

➤ **Phishing and Social Engineering:**

Phishing attacks remained prevalent, with cybercriminals using increasingly sophisticated methods to trick individuals into divulging sensitive information or clicking on malicious links.

- Email phishing. Most phishing attacks are sent by email.
- Spear phishing. There are two other, more sophisticated, types of phishing involving email.
- Whaling. Whaling attacks are even more targeted, taking aim at senior executives.
- Smising and vishing.
- Angler phishing.



➤ **Remote Work Vulnerabilities:**

The COVID-19 pandemic forced many organizations to shift to remote work, creating new opportunities for cybercriminals to exploit vulnerabilities in remote work setups.

- o Weaker security controls. ...
- o Sensitive data accessed through unsecured Wi-Fi networks.
- o Personal devices used for work. ...
- o The public places issue. ...
- o Weak passwords. ...
- o The practice of unencrypted file sharing.

➤ **Insider Threats:**

Insider threats, where employees or trusted individuals intentionally or unintentionally compromise data or systems, continued to be a concern.

This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities. External stakeholders and customers of the Cybersecurity and Infrastructure Security

CISA defines insider threat as the threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the department's mission, resources, personnel, facilities, information, equipment, networks, or systems. This threat can manifest as damage to the department through the following insider behaviors:

- o Espionage
- o Terrorism
- o Unauthorized disclosure of information
- o Corruption, including participation in transnational organized crime
- o Sabotage
- o Workplace violence

Intentional or unintentional loss or degradation of departmental resources or capabilities



2.3 HOW TO PREVENT FINANCE SECTOR FROM CYBER ATTACK

- Financial institutions experienced a 74% increase in cyber threats. Limited staffing and investment in cyber security contributed to security struggles. Financial sector groups can benefit from rethinking cyber security frameworks.
- Current digital data protections may enable organizations to meet regulatory requirements, however, additional methodologies can also provide a high degree of utility. Although there's no "silver bullet" when it comes to stopping threats, here are easy-to-implement security protocols that you can quickly layer in order to mitigate risk for financial institutions.
- How to secure financial institutions' accounts. Multi-factor authentication (MFA). Organizations can implement multi-factor authentication protocols to help thwart threats. MFA systems function as core elements of identity and access management models.
- Consider dual and triple controls. In some organizations, one person creates a financial transaction, a second person approves it and a third person hits "send" to enable the transaction to go through. This allows for organizations to maintain a greater level of control over interactions.
- Raise fraud awareness. Provide employees with greater levels of education surrounding financial fraud. Corporate accounts can be taken over, employees' desktops can be accessed remotely, and ransomware represents a very clear and present risk.
- Reconcile transactions regularly. By reconciling accounts either at the start of the day or at the close of the day, organizations can more easily spot activity that may not be legitimate. Experts state that the longer the length of time between the fraud attempt and identification of the issue, the less likely you are to be able to recover stolen funds.
- Transaction limits. Your banking institution may retain daily limits for card users. However, in recent years, some institutions have done away with this measure. Consider calling your banking institution and requesting for them to monitor transactions either above or below a certain dollar amount.
- How to secure financial institutions' data & Monitor security. Ensure that your organization retains tools that allow for comprehensive visibility into systems. This will allow IT admins to effectively monitor security. PCI DSS requires security solution implementation; however, organizations can always seek out higher-quality tools. Enable your IT personnel to do more.
- Threat detection tools. Consider a more robust set of endpoint security tools. Tracking endpoint security can be a huge hassle without the right types of security solutions. Talk to your CIO about reassessing existing tools and investing in new ones.

- Incident response. Your organization obviously maintains an incident response plan. But has it been updated recently? Tested in “drill mode” at different times of day, with different staff members on-hand?
- Zero-trust network model. While zero-trust has existed for quite some time by now, not all organizations have adopted it. Layering zero-trust policies into your security architecture can limit liabilities in the event of a network intrusion.
- Third-party risk management. Accurately assessing third-party cyber security and compliance measures is tough. Ensure that your organization engages in due diligence. This can reduce account takeovers, corporate data theft, vendor bankruptcy and other destructive debacles.



CASE STUDIES

Case Study : 1

The fraud of ABG Shipyard (2022)

ABG Shipyard Limited has been accused of participating in one of the largest bank fraud to date in the nation by CBI. The defendants are accused of stealing Rs 228.42 billion from 27 other lenders, including SBI and several arrests have been made by CBI has made in relation to this case. The proprietors of the business are allegedly responsible for misappropriation, mischief, embezzlement, and abuse of public trust for the period 2012-17. In July 2016, the loan account was identified as a non-performing asset, and fraud was discovered in 2019. On November 8, 2019, SBI filed its initial grievance. The bank re-filed their case in August 2020.

Case Study : 2

Scam at Punjab National Bank (2018)

The Punjab National Bank received a scam notice in 2018 involving Rs 114 billion. The heist was at the time described as the biggest in the history of Indian banking. Jeweler Nirav Modi, Ami Modi, Nishant Modi, Mehul Choksi and several staff members of PNB, were some of the primary defaulters that were found. A junior PNB staff members illegally fabricated "letters of undertaking" in order to obtain short-term loans from foreign branches of banks in to reimburse the vendors. Hence, the payments were never recorded in the bank's primary system as a result and PNB's higher management failed to notify the fraud. A total of Rs 114 billion was stolen from 30 Indian banks' overseas branches by the Nirav Modi and Gitanjali businesses. Investigation by CBI led to the discovery of the scam. Just few days before the theft was revealed, Modi departed India. He was charged with criminal conspiracy by the Indian government, along with financial fraud, embezzlement, fraud, and contract violation in the PNB case in August 2018. In southwest London's Wandsworth Prison, Modi is now detained.



SUMMARY

The growing dependence on technology and the Internet has led to increased cybercrime threats, particularly in the financial sector. Cyberattacks such as ransomware, supply chain attacks, phishing, and insider threats are on the rise. To safeguard financial institutions, it is essential to implement measures like multi-factor authentication, transaction limits, fraud awareness, and robust data security practices. Monitoring, threat detection tools, and incident response plans are crucial for timely threat identification and mitigation. Embracing a zero-trust network model and conducting thorough third-party risk assessments can further enhance security. These measures are imperative in an environment where cyber incidents can disrupt services, erode trust, and have far-reaching economic implications, as evidenced by recent cyberattacks on financial entities.



REFERENCES

- 1 https://www.findevgateway.org/sites/default/files/publications/files/cyber_security_paper_november2019.pdf
- 2 <https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm>
- 3 https://www.researchgate.net/publication/326774451_Recent_Trends_in_the_Era_of_Cybercrime_and_the_Measures_to_Control_Them
- 4 <https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1154&context=ijcic>
- 5 <https://www.proofpoint.com/us/threat-reference/ransomware>
- 6 <https://www.techtarget.com/searchsecurity/definition/supply-chain-attack>
- 7 <https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats>

CHAPTER 3

MODUS OPERANDI IN CYBER CRIMES



LEARNING OBJECTIVES

- To understand modus operandi cybersecurity
- To understand the Case study
- To understand the type of attack-vector in cyber-Crime
- To understand the type of attack-vector in cyber fraud
- To understand scenario of cyber attempt

3.1 INTRODUCTION

Modus Operandi the typical or characteristic methods that cybercriminals or threat actors employ to execute their attacks and achieve their malicious objectives.

Some of the modus operandi followed by the fraudsters and criminals through investment / part time job / Ponzi schemes, wherein the transactions are routed through the Finance/banking channels are given here under:

At a minimum, every Modus Operandi will contain elements that involve the following:

- 1 Ensure success of the crime;
- 2 Protect and identity
- 3 Effect Escape

It is a learned behavior like any other behavior, and involves things like experience, education, and maturity.

This study analyzed cyber-crime, highlighting the wide spectrum of cyberattacks that occurred around the world.

The modus operandi of cyberattack campaigns was revealed by analyzing and considering cyberattacks in the context of major world events.



3.2 CASE STUDY

Following what appeared to be substantial gaps between the initial breakout of the virus and social engineering cyber-attack, the investigation indicates how attacks became significantly more frequent over time, to the point where three or four different cyber-attacks were reported on certain days.

This study contributes in the direction of fifteen types of cyber-attacks which were identified as the most common pattern and its ensuing devastating events during the global Cyber fraud crisis.

The data was generated between March 2020 and December 2021, from a global survey through online contact and responses, especially from different organizations and business executives.

The results show differences in cyber-attack techniques; as hacking attacks were the most frequent with a record of 330 out of 895 attacks, accounting for 37%. Next was Spam emails attack with 13%; emails with 13%; followed by malicious domains with 9%. Mobile apps followed with 8%, Phishing was 7%, Malware 7%, Browsing apps with 6%, DDoS has 6%, Website apps with 6%, and MSMM with 6%. BEC frequency was 4%, Ransomware with 2%, Botnet scored 2% and APT recorded 1%.

The study recommends that it will continue to be necessary for governments and organizations to be resilient and innovative in cybersecurity decisions to overcome the current and future effects of the pandemic or similar crisis, which could be long-lasting. Hence, this study's findings will guide the creation, development, and implementation of more secure systems to safeguard people from cyber-attacks.

In the year 2020, there was about 1001 frequency of data breaches in the United States.

As a result, over 155.8 million people were affected by data breaches in the same year. According to the Identity Theft Resource Center's (ITRC) data breach study, there were 1,291 data breaches between September 2020 and September 2021. Compared to the 1,108 data breaches reported in 2019, this statistic represents an 8 percent rise. The trend of compromise between 2016 and 2021 is highlighted in

In the year 2020, in the wake of the COVID-19 crisis, there were about 1,872 breaches, compared to 1,108 in 2019.

However, in the first quarter of 2022, data compromises caused by physical attacks such as document or device theft and skimming devices fell to single digits (3), totaling 404.

In the aftermath of the COVID-19 pandemic, cyber security concerns have arisen from various quarters. In the past two years, the COVID-19 pandemic has been making headlines worldwide.

In this context, on April 8, 2020, the US Department of Homeland Security (DHS), the UK's National Cyber Security Centre (NCSC), and the Cybersecurity & Infrastructure Security Agency (CISA) issued a joint advisory describing how the COVID-19 pandemic was being exploited by cybercriminals and APT organizations (Deloitte, 2020).

Concerns about phishing, malware and other attacks on communication networks were addressed in this advisory from organizations, such as Microsoft Teams and Zoom.

In recent years, industrial espionage has grown with the help of the internet and lax cybersecurity practices, though such acts have become easier to detect. Social media is a new frontier for industrial espionage and its full impact and utility are still being measured. Penalties for industrial espionage can be significant, as seen in 1993 when Volkswagen stole trade secrets from General Motors which led to a \$100 million fine.

Dani Data App Scam Case Study

Introduction

The Dani Data app scam is a cautionary tale about the dangers of investing in unregulated apps and websites. The app promised users high returns on their investments in football betting, but it was actually a Ponzi scheme that defrauded thousands of people out of their money.

The scam began in December 2021, when the Dani Data app was launched by a Chinese national named Woo Uyanbe. The app claimed to use artificial intelligence to predict the outcomes of football matches, and it offered users the opportunity to invest in these predictions. The app quickly gained popularity, and by June 2022, it had over 1,200 users who had invested a total of Rs. 1,400 crore (about US\$180 million).

How the Scam Worked

The Dani Data app scam worked like a typical Ponzi scheme. The operators of the app would use the money from new investors to pay out profits to existing investors, creating the illusion of a successful investment. This allowed them to attract even more investors, who would then be used to pay out the profits to the earlier investors.

The scam eventually collapsed when the number of new investors dwindled. The operators of the app then disappeared with the money, leaving the investors with nothing.

The Victims of the Scam

The Dani Data app scam affected thousands of people across India. The victims were from all walks of life, including young people, professionals, and retirees. Many of the victims had saved their life savings for retirement, and they were left devastated by the loss.

The Lessons Learned

The Dani Data app scam is a reminder of the importance of doing your research before investing your money. Investors should always be wary of any investment that promises high returns with little or no risk. They should also only invest in regulated apps and websites.

The following are some of the key lessons that can be learned from the Dani Data app scam:

- Be wary of any investment that promises high returns with little or no risk.
- Do your research before investing your money.
- Only invest in regulated apps and websites.
- Be suspicious of any investment that requires you to make a large upfront payment.
- Be aware of the signs of a Ponzi scheme, such as the use of fake testimonials and the promise of guaranteed returns.

How to Protect Yourself

There are a few things you can do to protect yourself from becoming a victim of a Ponzi scheme:

- Do your research. Before investing in any app or website, make sure to do your research and understand the risks involved.
- Only invest in regulated apps and websites. This means that the app or website has been registered with the appropriate authorities and is subject to their regulations.
- Be suspicious of any investment that requires you to make a large upfront payment. Ponzi schemes often require investors to make large upfront payments, which is a red flag.
- Be aware of the signs of a Ponzi scheme. These include the promise of high returns with little or no risk, the use of fake testimonials, and the lack of transparency about how the investment works.

Conclusion

The Dani Data app scam is a reminder of the dangers of investing in unregulated apps and websites. By learning from this scam, we can help to protect ourselves and others from becoming victims of this type of fraud.

In addition to the above, here are some other things to keep in mind when investing:

- Never invest money that you cannot afford to lose.
- Be patient. Don't expect to get rich quick.
- Diversify your investments. Don't put all your eggs in one basket.
- Get professional advice. If you're not sure about an investment, talk to a financial advisor.



3.3 MODUS OPERANDI IN CYBER CRIMES

The advertisements / SMS messages usually contain a link, prompting for chat. Mobile applications, bulk SMS messages, SIM-box-based Virtual Private Network (VPNs), phishing websites, cloud services, virtual accounts in banks, Application Programming Interfaces (APIs), etc. are used to carry out financial frauds.

3.3.1 THE METHOD ACQUIRED BY ANY CRIMINAL FOR THE SUCCESSFUL COMMISSION OF A CRIME

A Infringement of Privacy:

Mishandling private information, such as customer passwords or social security numbers, can compromise user privacy, and is often illegal.

Privacy violations occur when:

- Private user information enters the program.
- The data is written to an external location, such as the console, file system, or network.
- Private data can enter a program in a variety of ways.
- Directly from the user in the form of a password or personal information.
- Accessed from a database or other data store by the application
- Indirectly from a partner or other third party

B Economic & industrial Espionage

Industrial espionage describes a series of covert activities in the corporate world such as the theft of trade secrets by the removal, copying, or recording of confidential or valuable information in a company. The information obtained is meant for use by a competitor. Industrial espionage may also involve bribery, blackmail, and technological surveillance.

Also referred to as corporate spying or espionage or economic espionage, industrial espionage is most associated with technology-heavy industries—particularly the computer, biotechnology, aerospace, chemical, energy, and auto sectors—in which a significant amount of money is spent on research and development (R&D).

The world's biggest practitioners of industrial espionage correspond to companies in countries with the biggest economies. One of the reasons why corporations engage in industrial espionage is to save time as well as huge sums of money. After all, it can take years to bring products and services to market—and the costs can add up.

C Computer Sabotage and Computer Extortion

Sabotage is deliberate damage to equipment. Infecting a website with malware is an example of information sabotage. A more extreme example is causing the power grid in a nation to go down.

Cyber extortion is a crime involving an attack or threat of an attack coupled with a demand for money or some other response in return for stopping or remediating the attack. Cyber extortion attacks are about gaining access to an organization's systems and identifying points of weakness or targets of value

D Electronic Money Laundering & Tax Evasion

- Electronic funds transfers have assisted in concealing and in moving the proceeds of crime. Emerging technologies will greatly assist in concealing the origin of ill-gotten gains.
- Legitimately derived income may also be more easily concealed from taxation authorities. Large financial institutions will no longer be the only ones with the ability to achieve electronic funds transfers transiting numerous jurisdictions at the speed of light.
- The development of informal banking institutions and parallel banking systems may permit central bank supervision to be bypassed but can also facilitate the evasion of cash transaction reporting requirements in those nations which have them.
- Traditional underground banks, which have flourished in Asian countries for centuries, will enjoy even greater capacity using telecommunications.
- With the emergence and proliferation of various technologies of electronic commerce, one can easily envisage how traditional countermeasures against money laundering and tax evasion may soon be of limited value.
- I may soon be able to sell you a quantity of heroin, in return for an untraceable transfer of stored value to my "smart card", which I then download anonymously to my account in a financial institution situated in an overseas jurisdiction which protects the privacy of banking clients. I can discreetly draw upon these funds as and when I may require, downloading them back to my stored value card (Wahlert 1996)."

E Child Pornography

- Child pornography is a form of child sexual exploitation. Federal law defines child pornography as any visual depiction of sexually explicit conduct involving a minor (persons less than 18 years old).
- Images of child pornography are also referred to as child sexual abuse images.
- Federal law prohibits the production, distribution, importation, reception, or possession of any image of child pornography.
- A violation of federal child pornography laws is a serious crime, and convicted offenders face fines severe statutory penalties.

F Unauthorized access

Unauthorized Access is when a person who does not have permission to connect to or use a system gains entry in a manner unintended by the system owner. The popular term for this is "hacking".

How did this happen?

The specifics are different for each individual event, but it could happen in any number of ways. Usually, access is gained via unpatched software or other known vulnerabilities.

What should I do?

The University will notify you in some manner of the incident and provide you with more detailed information about the incident. The university encourages all persons impacted by an Unauthorized Access incident to contact one of the three credit reporting agencies to place a 90-day fraud alert on their credit report. If there is reason to believe more stringent action should be taken, it will be noted in the letter (or other notification) you receive.

3.3.2 THE METHOD ACQUIRED BY ANY CRIMINAL FOR THE SUCCESSFUL COMMISSION OF A FRAUD

- **Sending Annoying Messages:**

With the advent of technology and globalization smartphones and computers have become very handy. But each and every coin is two faced. The beneficiary side of technology is better communication, time harvesting and many more but at the same time often people are exploited by others by sending annoying and harassing messages either in the form of text i.e., SMS or in the form of multimedia content i.e., MMS.

- **Text Message:**

Annoying, Insulting, Misleading, Defaming messages are often sent using mobile phones in bulk. Hence the actual source could not be fixed.

- o Such messages are often a cause of misperception among people of different races, cultures and traditions many times, often resulting in fights or riots.
- o Unaware and innocent people often fall in traps of cyber criminals for SMS of lottery, Emails of prize money, false promise of jobs, and false mail for admission in reputed colleges.
- o Frequently Credit card details of the victim along with other credentials are gathered by the cyber-criminal by falsely luring them on the grounds of winning a huge amount of money

- **Making Offensive Calls:**

Offenders can also harass others by making offensive calls to them and annoying them. Many a time anonymous calls are used by the criminals as an effective tool in making extortion or threatening calls.

Females are often harassed by stalkers by this means of communication.

- **WEB Based Calls:**

Calls can be made by spoofing the mobile number using various sites.

Such calls are intended to hide the actual location of the caller and any fake or annoying calls are made. Such calls are often used for terrorist activity and for trafficking illegal goods or for any ransom or blackmailing purposes.

- **Identity Theft:**

It involves stealing the identity of a person by dishonest use of someone's electronic signature, password, or other unique identifying features.

It includes credit card fraud, Online Share trading scams, e-banking crimes, fraudulent transactions, etc.

- **Financial Attack**

Offenders often clones the web page of a bank or any organizing or social site in the name of enhancing their security or updating their services or creating a fake webpage in the place of genuine, which is a look alike page of original, in order to collect personnel information at various stage and abuses the information and abuse the information for causing wrongful loss, fraudulent transfer of funds in internet banking.

- **WEB Page Hacking**

Hacking can be termed as unauthorized access to any electronic media of communication. In this method the genuine page of a web site is mutilated by altering the content of the file and appearance causing embarrassment to any reputed firm and may lead to denial of service, causing a heavy loss.

- **Phishing:**

Cybercriminals send deceptive emails or messages to trick recipients into revealing sensitive information or clicking on malicious links. These emails often impersonate legitimate entities, such as banks or trusted organizations.

- **Malware Attacks:**

Malicious software (malware) is used to compromise systems, steal data, or gain unauthorized access. Malware may be delivered via infected attachments, malicious websites, or compromised software.

- **Ransomware:**
Cybercriminals use ransomware to encrypt a victim's data, demanding a ransom for decryption. Typically, ransomware is delivered through phishing emails or exploiting vulnerabilities.
- **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks:**
Attackers flood a target system or network with an overwhelming amount of traffic, rendering it unavailable to users. DDoS attacks involve multiple compromised devices working together.
- **Insider Threats:**
Malicious or negligent insiders within an organization can pose significant security risks. These insiders may steal data, intentionally compromise systems, or inadvertently cause security incidents.
- **Credential Theft:**
Cybercriminals steal usernames and passwords, often through phishing or credential stuffing attacks. Once obtained, these credentials can be used for unauthorized access to various accounts.



- **Zero-Day Exploits:**
Exploiting unpatched vulnerabilities in software or hardware that are not yet known to the vendor or public. Attackers use these vulnerabilities to gain unauthorized access or deliver malware.
- **Social Engineering:**
Manipulating individuals into divulging confidential information or performing actions that compromise security.
Tactics may include pretexting, baiting, or tailgating.

- **Supply Chain Attacks:**
Cybercriminals target a supplier or third-party partner to compromise the security of the target organization. This can involve injecting malware into software updates or compromising the supply chain.
- **Advanced Persistent Threats (APTs):**
APTs are long-term, highly sophisticated attacks often associated with nation-state actors. Attackers maintain persistence in the target network, gather intelligence, and stealthily exfiltrate data.
- **IoT and Botnet Attacks:**
Attackers compromise Internet of Things (IoT) devices to create botnets for various malicious purposes, such as DDoS attacks. Weak security in IoT devices is often exploited.
- **Crypto Jacking:**
Cybercriminals secretly use victims' computing resources to mine cryptocurrencies. This can slow down the victim's system and increase energy costs.

3.3.3 SCENARIO

The report even throws light on the status of account for the past one year—a detailed view on the present status of the applicant – Diagram below depicts the same

- A** Earn Online', 'Part Time Job', etc. are the key words used by fraudsters and criminals to match their advertisements. Such advertisements are generally displayed from 10 am to 7 pm, i.e., the peak time for internet use by Indian public.
 - o These websites used by fraudsters generally have domains – 'xyz' and 'Wix site'. These sites either redirect to a messaging platform or to a website which has embedded messaging platform link which, on clicking, again redirects to a chat.
- B** Multiple Indian numbers were used for communications with victims. On analysis, it was observed that the mobile number holder was not aware of the messaging platform being operated in his / her name.

In some cases, the mobile number holder knowingly shares OTP in return for some money from the fraudsters.

- C** The fraudster sends an investment link over chat. Each person has a referral code. Fraudster generally communicates in English. Google Translate is also used to communicate with the victims.

- D** A screenshot needs to be sent to the person over the messaging platform to activate the account. Once the account is activated, a task is given to the user to gain confidence of the person.
- o Mandatory condition to do a task is to load money through Payment Gateways which are not authorized to operate in India.
All payments are made through UPI. Some of the UPI addresses belong to companies registered with the Ministry of Corporate Affairs (MCA). Generally, a call center is used to interact with the victims for communication regarding tasks.
 - o For instance, on failure to load funds on investment website, the call center executive initiates a call.
- E** Once the task is completed, the victim is asked to withdraw the money. Money is withdrawn through various Payment Aggregators.
- F** On getting the first refund, the victim is now lured to do more tasks which involve loading more money.
- o The process continues and once a big amount is loaded by the victim, the person (fraudster) stops responding over chat.
 - o UPI details are updated daily on fraudulent websites. Investment websites keep changing. Source code remains the same but domain changes.
- G** Bank accounts opened by money mules using real / fake identification are used to receive stolen funds from compromised bank accounts, through sharing of OTPs, etc. Rented accounts are sourced by agents and account owners (money mules) are given fixed rent or commission or lumpsum amount for the account.
- H** Layering of transactions is carried out by account-to-account transfers. Bulk payments / APIs are also used for this.
- I** From the intermediate account, money is diverted to multiple sources / assets like crypto currencies, bullion, payout accounts (for gaining confidence and hiding laundering), foreign money transfer, person-to-person transfer, etc.
- J** Instances have been observed where Shell Companies with dummy directors, rented companies with MCA registration certificates, fintech companies, payment gateways, SMS aggregators are reported to be involved in carrying out such financial frauds, mostly using UPI as payment mode.

Main objective of opening Shell Companies is to create a current account or a fintech company for accepting or paying out proceeds of frauds. Most of these Shell Companies appear to be Technology Companies.

- K** UPI addresses are used to create layering behind Payment Aggregators thereby facilitating end of day settlement.

- L** Aggregator on aggregator concept is used by these players (fraudsters) in order to conceal their identities.
 - o The merchants onboarded on the fintech players (E.g., ABC company onboarded on Payment Aggregator) are frauds.
 - o The network of fraudsters starts creating Payment Aggregator business in collaboration with banks directly or with other fintech companies.
 - o The fraudster would be sitting behind the payment aggregator as sub-aggregator or directly as a merchant.
 - o The money collected by the fraudsters, as sub-aggregator and / or as merchant, is remitted to the Payment Aggregator wherefrom the API (app) based payouts take place.
 - o After the aggregator network is set-up, the accounts are operated for making the payouts by the fraudsters based outside India.

- M** Gold, crypto currencies, international money transfers are observed by LAW Enforcement Agencies (LEAs) to be usual termination points of the fraud trials.

The Federal Bureau of Investigation (FBI) refers to this type of scam as “BEC,” or “Business Email Compromise.” It defines it as “a sophisticated scam targeting firms that engage with international suppliers and/or make frequent wire transfer payments.”

The fraud is carried out by using computer intrusion or social engineering tactics to compromise legitimate company email accounts to make illicit financial transfers”.

- **Deceptive phishing:** The most common phishing fraud is deceptive phishing. Fraudsters pose as a real company to obtain people’s personal information or login passwords. Attacks and a sense of urgency are used in these emails to terrify recipients into doing what the attackers want.

- **Phishing based on malware.** This technique occurs when a thief attaches a destructive computer program that appears to be useful to websites, emails, and other electronic documents on the Internet. Phishing based on malware or Malware based phishing is a form of a computer program that is also known as malware.

- **Phone phishing or voice phishing** is the practice of making false phone calls in order to dupe individuals into donating money or divulging personal information. It’s a new label for a problem that’s been around for a long time: phone scams. A common phishing method is for a criminal to pose as a trustworthy institution, organization, or government agency.

- **Pharming attack** is a type of cyberattack in which users are directed to a false website that appears to be a genuine website. When users type in a legitimate web URL, they are led to a false website that looks exactly like the original one.
- **Phishing websites:** A phishing website is a domain with a name and appearance similar to an official website.

They are designed to deceive someone into thinking it's real. Some pointers on how to spot a phishing website include

Remediation:

- a visiting the website directly,
- b avoiding pop-ups and insecure sites.
- c keeping a close eye on the URL or web address.
- d entering a fictitious password.
- e examine the website's content and design.
- f looking at online reviews and the payment options available on a website.



SUMMARY

The introduction delves into the concept of modus operandi, the characteristic methods employed by cybercriminals to execute their attacks. It emphasizes the importance of understanding these methods for combating cybercrime, highlighting that modus operandi involves factors like experience, education, and maturity.

The case study section discusses the rise in cyberattacks, especially during the COVID-19 pandemic, and identifies fifteen common types of cyberattacks. The data is drawn from a global survey conducted between March 2020 and December 2021, showing that hacking attacks were the most prevalent at 37%, followed by spam emails, phishing, and malware. The study emphasizes the need for resilient and innovative cybersecurity measures in the face of ongoing and future crises.

The Dani Data app scam case study serves as a cautionary tale about the dangers of investing in unregulated apps, detailing how a Ponzi scheme defrauded thousands of people out of their money. It emphasizes the importance of research, regulation, and vigilance when considering investments.

In the modus operandi in cybercrimes section, various methods used by cybercriminals for successful commission of crimes and frauds are outlined. These include computer viruses, identity theft, economic and industrial espionage, computer sabotage, electronic money laundering, and more.

The scenario section provides a detailed overview of how cybercriminals conduct financial frauds through deceptive practices, including messaging platforms, UPI payments, shell companies, and aggregator networks. It sheds light on the complex web of operations these criminals employ to hide their identities and launder money.

Overall, this comprehensive summary highlights the diverse methods and challenges associated with combating cybercrime and underscores the importance of cybersecurity measures and awareness for individuals and organizations.



REFERENCES

- 1 <https://www.digicert.com/faq/vulnerability-management/>
- 2 <https://www.justice.gov/criminal-ceos>
- 3 <https://owasp.org/www-community/vulnerabilities/>
- 4 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9367180/>
- 5 <http://epgp.inflibnet.ac.in/>
- 6 <https://www.indusind.com/>
- 7 <https://www.igi-global.com/chapter/modus-operandi-in-cybercrime/248041>
- 8 <https://security.tennessee.edu/>
- 9 <https://www.swift.com/news-events/news/modus-operandi-cyber-attack>
- 10 <https://www.investopedia.com/terms/i/industrial-espionage.asp>
- 11 <http://g32cybercrimecomp1220uwi.weebly.com/>

CHAPTER 4

IMPORTANCE OF DIGITAL FORENSICS & ETHICAL HACKING



LEARNING OBJECTIVES

- Understanding of Digital Forensics
- Understanding the importance of Digital Forensics
- Exploring Ethical Hacking
- Understanding Ethical hacking Fundamentals

4.1 DIGITAL FORENSIC

Digital forensics or digital forensic science is a branch of cybersecurity focused on the recovery and investigation of material found in digital devices and cybercrimes. Digital forensics was originally used as a synonym for computer forensics but has expanded to cover the investigation of all devices that store digital data. As society increases reliance on computer systems and cloud computing, digital forensics becomes a crucial aspect of law enforcement agencies and businesses.

Digital forensics is concerned with the identification, preservation, examination and analysis of digital evidence, using scientifically accepted and validated processes, to be used in and outside of a court of law. Today, the technical aspect of an investigation is divided into five branches that encompass the seizure, forensic imaging and analysis of digital media.



4.2 PURPOSE OF DIGITAL FORENSICS

The most common use of digital forensics is to support or refute a hypothesis in a criminal or civil court:

- **Criminal cases:** Involve the alleged breaking of laws and law enforcement agencies and their digital forensic examiners.
- **Civil cases:** Involve the protection of rights and property of individuals or contractual disputes between commercial entities where a form of digital forensics called electronic discovery (eDiscovery) may be involved.

Digital forensics experts are also hired by the private sector as part of cybersecurity and information security teams to identify the cause of data breaches, data leaks, cyber-attacks and other cyber threats. Digital forensic analysis may also be part of incident response to help recover or identify any sensitive data or personally identifiable information (PII) that was lost or stolen in a cybercrime.

- **Quick sorting** - You can quickly sort your data by using the A-Z and Z-A Sort buttons on the Ribbon's Data tab
- **Sort Dialog Box** - You can also sort on various criteria through Sort Dialog Box

4.3 USE OF DIGITAL FORENSICS

Digital forensics is used in both criminal and private investigations. Traditionally, it is associated with criminal law where evidence is collected to support or negate a hypothesis before the court. Collected evidence may be used as part of intelligence gathering or to locate, identify or halt other crimes. As a result, data gathered may be held to a less strict standard than traditional forensics. In civil cases, digital forensics may help with electronic discovery (eDiscovery). A common example is following unauthorized network intrusion. A forensics examiner will attempt to understand the nature and extent of the attack, as well as try to identify the attacker. As encryption becomes more widespread, forensic investigation becomes harder, due to the limited laws compelling individuals to disclose encryption keys.

4.4 DIGITAL FORENSIC INVESTIGATION PROCESS

There are a number of process models for digital forensics, which define how forensic examiners should gather, process and analyze data. That said, digital forensics investigations commonly consist of four stages:

- 1 **Seizure:** Prior to actual examination digital media is seized. In criminal cases, this will be performed by law enforcement personnel to preserve the chain of custody.
- 2 **Acquisition:** Once exhibits are seized, a forensic duplicate of the data is created. Once created using a hard drive duplicator or software imaging tool, then the original drive is

returned to secure storage to prevent tampering. The acquired image is verified with SHA1 or MD5 hash functions and will be verified again throughout analysis to verify the evidence is still in its original state.

- 3 Analysis:** After acquisition, files are analyzed to identify evidence to support or contradict a hypothesis. The forensic analyst usually recovers evidence material using a number of methods (and tools), often beginning with the recovery of deleted information. The type of data analyzed varies but will generally include email, chat logs, images, internet history and documents. The data can be recovered from accessible disk space, deleted space or from the operating system cache.
- 4 Reporting:** Once the investigation is complete, the information is collated into a report that is accessible to non-technical individuals. It may include audit information or other meta documentation.

4.5 THE LEGAL CONSIDERATIONS OF DIGITAL FORENSICS

The examination of digital media is covered by national and international legislation. For civil investigations, laws may restrict what can be examined. Restrictions against network monitoring or reading personal communications are common.

Likewise, criminal investigations may be restricted by national laws that dictate how much information can be seized. As an example, seizure of evidence by law enforcement is governed by the PACE act in the United Kingdom. The 1990 computer misuse act legislates against unauthorized access to computer material which makes it hard for civil investigators in the UK. One of the common considerations which is largely undecided is an individual's right to privacy. The US Electronic Communications Privacy Act places limitations on the ability for law enforcement and civil investigators to intercept and access evidence.

The act makes a distinction between stored communication (e.g., email archives) and transmitted communication (e.g., VOIP). Transmitted communication is considered more of a privacy invasion and is harder to obtain a warrant for.

Digital evidence falls into the same legal guidelines as other evidence.

In general, laws dealing with digital evidence are concerned with:

- **Integrity:** Ensuring the act of seizing and acquiring digital media does not modify the evidence (either the original or the copy).
- **Authenticity:** The ability to confirm the integrity of information. The chain of custody from crime scene through analysis and ultimately to the court, in the form of an audit trail, is an important part of establishing the authenticity of evidence. Each of the branches of digital forensics have their own guidelines on how to conduct investigations and handle data.

4.6 DIFFERENT BRANCHES OF DIGITAL FORENSICS

Digital forensics is no longer synonymous with computer forensics. It is increasingly concerned with data from other digital devices such as tablets, smart phones, flash drives and even cloud computing.

In general, we can break digital forensics into five branches:

- 1 Computer Forensics**
- 2 Mobile Device Forensics**
- 3 Network Forensics**
- 4 Forensic Data Analysis**
- 5 Database Forensics**

1 Computer Forensics

Computer forensics or computer forensic science is a branch of digital forensics concerned with evidence found in computers and digital storage media. The goal of computer forensics is to examine digital data with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about digital information. It is used in both computer crime and civil proceedings. The discipline has similar techniques and principles to data recovery, with additional guidelines and practices designed to create a legal audit trail with a clear chain of custody. Evidence from computer forensics investigations is subjected to the same guidelines and practices as other digital evidence.

2 Mobile Device Forensics

Mobile device forensics is a branch of digital forensics focused on the recovery of digital evidence from mobile devices using forensically sound methods. While the phrase mobile device generally refers to mobile phones, it can relate to any device that has internal memory and communication ability including PDA devices, GPS devices and tablets. While the use of mobile phones in crime has been widely recognized for years, the forensic study of mobile phones is a new field, beginning in the late 1990s.

The growing need for mobile device forensics is driven by:

- o Use of mobile phones to store and transmit personal and corporate information
- o Use of mobile phones in online transactions
- o That said, mobile device forensics is particularly challenging due to:
- o Evidential and technical challenges such as cell site analysis which makes it possible to determine roughly the cell site zone from which a call was made or received but not a specific location such as an address
- o Changes in mobile phone form factors, operating systems, data storage, services, peripherals and even pin connectors and cables
- o Storage capacity growth
- o Their proprietary nature

- o Hibernation behavior where processes are suspended when the device is off or idle as a result of these challenges, many tools exist to extract evidence from mobile devices. But no one tool or method can acquire all evidence from all devices. This has forced forensic examiners, especially those who wish to be expert witnesses, to undergo extensive training to understand how each tool and method acquires evidence, how it maintains forensic soundness and how it meets legal requirements.

4 Network Forensics

Network forensics is a branch of digital forensics focused on monitoring and analyzing computer network traffic for information gathering, legal evidence or intrusion detection. Unlike other branches of digital forensics, network data is volatile and dynamic. Once transmitted, it is gone so network forensics is often a proactive investigation.

Network forensics has two general uses:

- o Monitoring a network for anomalous traffic and identifying intrusions.
- o Law enforcement may analyze capture network traffic as part of criminal investigations.

5 Forensic Data Analysis

Forensic data analysis (FDA) is a branch of digital forensics that examines structured data in regard to incidents of financial crime. The aim is to discover and analyze patterns of fraudulent activities. Structured data is data from application systems or their databases. This can be contrasted to unstructured data that is taken from communication, office applications and mobile devices. Unstructured data has no overarching structure and analysis therefore means applying keywords or mapping patterns. Analysis of unstructured data is usually done by computer forensics or mobile device forensics experts.

6 Database Forensics

Database forensics is a branch of digital forensics related to databases and their related metadata. Cached information may also exist in a server's RAM requiring live analysis techniques. A forensic examination of a database may relate to timestamps that apply to the update time of a row in a relational database that is being inspected and tested for validity to verify the actions of a database user. Alternatively, it may focus on identifying transactions within a database or application that indicates evidence of wrongdoing, such as fraud.

4.7 CHALLENGES FACED BY DIGITAL FORENSICS

Development is severely challenged by the growing popularity of digital devices and the heterogeneous hardware and software being utilized.

- The increasing variety of file formats and OSs hampers the development of standardized DF tools and processes.
- The emergence of smart phones that increasingly utilize encryption renders the acquisition of digital evidence an intricate task.

Also, advancements in cybercrime have culminated in substantial challenges, such as

- Crime as a Service (CaaS), which provides the attackers with easy access to the tools, programming frameworks, and services needed to conduct cyber-attacks
- Digital forensics has become an important tool in the investigation/identification of computer based and computer-assisted crime.
- Eric Holder (Deputy Attorney General of the United States Subcommittee on Criminal Oversight for the Senate) has classified the challenges into three categories

1 Technical challenges

2 Legal challenges

3 Resource challenge

1 Technical challenges: Finding the forensics evidence have been hindered by:

- o Different Media format
- o Encryption
- o Anti-forensics
- o Steganography.
- o Live acquisition and analysis

2 Legal challenges:

- o Jurisdictional issue.
- o Lack of standard legislation creates the legal challenges.
- o Status as scientific evidence.
- o what is the known or potential rate of error of the method used.
- o whether the theory or method has been generally accepted by the scientific.

3 Resource challenges:

It is severely challenged by the growing popularity of digital devices and the heterogeneous hardware and software platforms being utilized.

- o Volume of data.
- o Time taken to acquire and analyze forensic media.
- o To ensure to satisfied critical investigative and prosecutorial needs at all levels of government

4.8 INFORMATION SECURITY

Information security is “the state of the well-being of information and infrastructure in which the possibility of theft, tampering, or disruption of information and services is kept low or tolerable.” Information security refers to the protection or safeguarding of information and information systems that use, store, and transmit information from unauthorized access, disclosure, alteration, and destruction.

Elements of Information Security

Information security relies on five major elements: confidentiality, integrity, availability, authenticity, and non-repudiation.

- **Confidentiality**
Confidentiality is the assurance that the information is accessible only to authorized. Confidentiality breaches may occur due to improper data handling or a hacking attempt. Confidentiality controls include data classification, data encryption, and proper disposal of equipment (such as DVDs, USB drives, etc.)
- **Integrity**
Integrity is the trustworthiness of data or resources in the prevention of improper and unauthorized changes—the assurance that information is sufficiently accurate for its purpose. Measures to maintain data integrity may include a checksum (a number produced by a mathematical function to verify that a given block of data is not changed) and access control (which ensures that only authorized people can update, add, or delete data).
- **Availability**
Availability is the assurance that the systems responsible for delivering, storing, and processing information are accessible when required by authorized users. Measures to maintain data availability can include disk arrays for redundant systems and clustered machines, antivirus software to combat malware, and distributed denial-of-service (DDoS) prevention systems.
- **Authenticity**
Authenticity refers to the characteristic of communication, documents, or any data that ensures the quality of being genuine or uncorrupted. The major role of authentication is to confirm that a user is genuine. Controls such as biometrics, smart cards, and digital certificates ensure the authenticity of data, transactions, communications, and documents.
- **Non-Repudiation**
Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Individuals and organizations use digital signatures to ensure non-repudiation.

Classification of Attacks

According to IATF, security attacks are classified into five categories: passive, active, close-in, insider, and distribution.

- **Passive Attacks**

Passive attacks involve intercepting and monitoring network traffic and data flow on the target network and do not tamper with the data. Attackers perform reconnaissance on network activities using sniffers. These attacks are very difficult to detect as the attacker has no active interaction with the target system or network. Passive attacks allow attackers to capture the data or files being transmitted in the network without the consent of the user. For example, an attacker can obtain information such as unencrypted data in transit, clear-text credentials, or other sensitive information that is useful in performing active attacks.

Examples of active attacks:

- Foot printing
- Sniffing and eavesdropping
- Network traffic analysis
- Decryption of weakly encrypted traffic

- **Active Attacks**

Active attacks tamper with the data in transit or disrupt communication or services between the systems to bypass or break into secured systems. Attackers launch attacks on the target system or network by sending traffic actively that can be detected. These attacks are performed on the target network to exploit the information in transit. They penetrate or infect the target's internal network and gain access to a remote system to compromise the internal network.

Examples of active attacks:

- **Denial-of-service (DoS) attack:** This is an attempt to make a computer system or network unavailable to its intended users. DoS attacks can be carried out by flooding the target with traffic, sending it invalid data, or exploiting a vulnerability in the system.
- **Malware attacks:** This is a broad term that encompasses any type of software that is designed to harm a computer system. Malware can include viruses, worms, ransomware, and trojan horses.
- **Spoofing attacks:** This is an attempt to gain unauthorized access to a computer system or network by posing as a legitimate user. Spoofing attacks can be carried out by using a fake IP address, email address, or other identifying information.
- **Password-based attacks:** This is an attempt to gain unauthorized access to a computer system or network by guessing or cracking passwords. Password-based attacks can be carried out manually or using automated tools.
- **Man-in-the-Middle attack:** This is an attack in which an attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other.

- **Denial-of-service (DoS) attack:** This is an attempt to make a computer system or network unavailable to its intended users. DoS attacks can be carried out by flooding the target with traffic, sending it invalid data, or exploiting a vulnerability in the system.
- **DNS and ARP poisoning:** This is an attack in which the attacker modifies the Domain Name System (DNS) or Address Resolution Protocol (ARP) tables of a network in order to redirect traffic to a malicious website or server.
- **Firewall and IDS attack:** This is an attack in which the attacker attempts to bypass or disable a firewall or intrusion detection system (IDS) in order to gain unauthorized access to a computer system or network.
- **Privilege escalation:** This is an attack in which an attacker gains unauthorized access to more privileges on a computer system or network than they are supposed to have. Privilege escalation attacks can be carried out by exploiting vulnerabilities in the system or by using social engineering techniques.
- **Backdoor access:** This is a way for an attacker to gain unauthorized access to a computer system or network that they have already compromised. Backdoors can be created by the attacker or by a system administrator.
- **Cryptography attacks:** This is an attack in which the attacker attempts to break the encryption that is used to protect data. Cryptography attacks can be carried out using brute-force methods or by exploiting vulnerabilities in the encryption algorithm.
- **SQL injection:** This is an attack in which the attacker injects malicious SQL code into a web application in order to gain unauthorized access to the application's data.
- **XSS attacks:** This is an attack in which the attacker injects malicious code into a web page or email message in order to exploit a vulnerability in the user's browser or email client.
- **Directory traversal attacks:** This is an attack in which the attacker attempts to access files or directories that they are not supposed to have access to. Directory traversal attacks can be carried out by exploiting vulnerabilities in the web application or operating system.



These are just some of the most common types of cyberattacks. There are many other types of attacks, and new attacks are being developed all the time. It is important to be aware of these attacks and to take steps to protect yourself from them.

Here are some tips for protecting yourself from cyberattacks:

- o Keep your software up to date. Software updates often include security patches that can help to protect you from attacks.
- o Use strong passwords and change them regularly.
- o Be careful about what information you share online.
- o Do not open suspicious emails or attachments.
- o Be careful about clicking on links in emails or on websites.
- o Use a firewall and antivirus software.
- o Back up your data regularly.

- **Insider Attacks**

Insider attacks are performed by trusted persons who have physical access to the critical assets of the target. An insider attack involves using privileged access to violate rules or intentionally cause a threat to the organization's information or information systems. Insiders can easily bypass security rules, corrupt valuable resources, and access sensitive information. They misuse the organization's assets to directly affect the confidentiality, integrity, and availability of information systems. These attacks impact the organization's business operations, reputation, and profit. It is difficult to figure out an insider attack.

Examples of insider attacks:

- o Eavesdropping and wiretapping
- o Theft of physical devices
- o Social engineering
- o Data theft and spoliation
- o Pod slurping
- o Planting keyloggers, backdoors, or malware

- **Distribution Attacks**

Distribution attacks occur when attackers tamper with hardware or software prior to installation. Attackers tamper with the hardware or software at its source or when it is in transit. Examples of distribution attacks include backdoors created by software or hardware vendors at the time of manufacture. Attackers leverage these backdoors to gain unauthorized access to the target information, systems, or network.

- o Modification of software or hardware during production
- o Modification of software or hardware during distribution

4.9 WHAT IS HACKING?

Hacking in the field of computer security refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to system resources. It involves a modifying system or application features to achieve a goal outside its creator's original purpose. Hacking can be done to steal, pilfer, or redistribute intellectual property, thus leading to business loss.

4.9.1 Hacker Classes/Threat Actors

Hackers usually fall into one of the following categories, according to their activities:

- **Black Hats:** Black hats are individuals who use their extraordinary computing skills for illegal or malicious purposes. This category of hacker is often involved in criminal activities. They are also known as crackers.
- **White Hats:** White hats or penetration testers are individuals who use their hacking skills for defensive purposes. These days, almost every organization has security analysts who are knowledgeable about hacking countermeasures, which can secure its network and information systems against malicious attacks. They have permission from the system owner.
- **Gray Hats:** Gray hats are the individuals who work both offensively and defensively at various times. Gray hats might help hackers to find various vulnerabilities in a system or network and, at the same time, help vendors to improve products (software or hardware) by checking limitations and making them more secure.

Insiders: An insider is any employee (trusted person) who has access to critical assets of an organization. An insider threat involves the use of privileged access to violate rules or intentionally cause harm to the organization's information or information systems. Insiders can easily bypass security rules, corrupt valuable resources, and access sensitive information. Generally, insider threats arise from disgruntled employees, terminated employees, and undertrained staff members.



4.9.2 UNDERSTAND DIFFERENT PHASES OF HACKING CYCLE

Hacking Phases

In general, there are five phases of hacking:

- 1 Reconnaissance**
- 2 Scanning**
- 3 Gaining Access**
- 4 Maintaining Access**
- 5 Clearing Tracks**

- **Reconnaissance**

Reconnaissance refers to the preparatory phase in which an attacker gathers as much information as possible about the target prior to launching the attack. In this phase, the attacker draws on competitive intelligence to learn more about the target. It could be the future point of return, noted for ease of entry for an attack when more about the target is known on a broad scale. The reconnaissance target range may include the target organization's clients, employees, operations, network, and systems.

This phase allows attackers to plan the attack. It may take some time as the attacker gathers as much information as possible. Part of this reconnaissance may involve social engineering. A social engineer is a person who convinces people to reveal information such as unlisted phone numbers, passwords, and other sensitive information. For instance, the hacker could call the target's Internet service provider and, using personal information previously obtained, convince the customer service representative that the hacker is actually the target, and in doing so, obtain even more information about the target. Searching for the target company's web site in the Internet's Whois database can easily provide hackers with the company's IP addresses, domain names, and contact information.

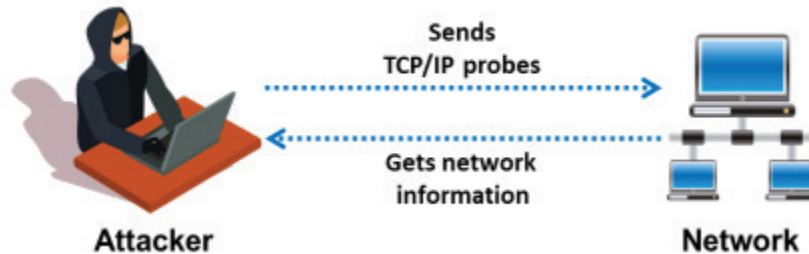
- **Scanning**

Scanning is the phase immediately preceding the attack. The attacker uses the details gathered during reconnaissance to scan the network for specific information. Scanning is a logical extension of active reconnaissance, and in fact, some experts do not differentiate scanning from active reconnaissance. There is a slight difference, however, in that scanning involves more in-depth probing on the part of the attacker. Often the reconnaissance and scanning phases overlap, and it is not always possible to separate the two. An attacker can gather critical network information such as the mapping of systems, routers, and firewalls by using simple tools such as the standard Windows utility Traceroute.

Scanning can include the use of dialers, port scanners, network mappers, ping tools, vulnerability scanners, or other tools. Attackers extract information such as live machines, port, port status, OS details, device type, and system uptime to launch an attack.

Port scanners detect listening ports to find information about the nature of services running on the target machines. The primary defense technique against port scanners is shutting down services that are not required and implementing appropriate port filtering. However, attackers can still use tools to determine the rules implemented by the port filtering.

The most commonly used tools are vulnerability scanners, which can search for thousands of known vulnerabilities on a target network. This gives the attacker an advantage because he or she only has to find a single means of entry, while the systems professional has to secure as much vulnerability as possible by applying patches. Organizations that use intrusion detection systems still have to remain vigilant because attackers can and will use evasion techniques wherever possible.



4.9.3 What is Ethical Hacking?

Ethical hacking is the practice of employing computer and network skills in order to assist organizations in testing their network security for possible loopholes and vulnerabilities.

White Hats (also known as security analysts or ethical hackers) are the individuals or experts who perform ethical hacking. Nowadays, most organizations (such as private companies, universities, and government organizations) are hiring White Hats to assist them in enhancing their cybersecurity.

They perform hacking in ethical ways, with the permission of the network or system owner and without the intention to cause harm. Ethical hackers report all vulnerabilities to the system and network owner for remediation, thereby increasing the security of an organization's information system.

Ethical hacking involves the use of hacking tools, tricks, and techniques typically used by an attacker to verify the existence of exploitable vulnerabilities in system security.

Today, the term hacking is closely associated with illegal and unethical activities. There is continuing debate as to whether hacking can be ethical or not, given the fact that unauthorized access to any system is a crime. Consider the following definitions:

- The noun “hacker” refers to a person who enjoys learning the details of computer systems and stretching their capabilities.
- The verb “to hack” describes the rapid development of new programs or the reverse engineering of existing software to make it better or more efficient in new and innovative ways.
- The terms “cracker” and “attacker” refer to persons who employ their hacking skills for offensive purposes.
- The term “ethical hacker” refers to security professionals who employ their hacking skills for defensive purposes.

Most companies employ IT professionals to audit their systems for known vulnerabilities. Although this is a beneficial practice, crackers are usually more interested in using newer, lesser-known vulnerabilities, and so these by-the-numbers system audits do not suffice. A company needs someone who can think like a cracker, keep up with the newest vulnerabilities and exploit and recognize potential vulnerabilities where others cannot. This is the role of the ethical hacker.

Ethical hackers usually employ the same tools and techniques as hackers, with the important exception that they do not damage the system. They evaluate system security, update the administrators regarding any discovered vulnerabilities, and recommend procedures for patching those vulnerabilities.

The important distinction between ethical hackers and crackers is consent. Crackers attempt to gain unauthorized access to systems, while ethical hackers are always completely open and transparent about what they are doing and how they are doing it. Ethical hacking is, therefore, always legal.



4.9.4 Why Ethical Hacking is Necessary

As technology is growing at a faster pace, so is the growth in the risks associated with it. To beat a hacker, it is necessary to think like one! Ethical hacking is necessary as it allows to counter attacks from malicious hackers by anticipating methods used by them to break into a system.

Ethical hacking helps to predict various possible vulnerabilities well in advance and rectify them without incurring any kind of outside attack. As hacking involves creative thinking, vulnerability testing, and security audits alone cannot ensure that the network is secure. To achieve security, organizations must implement a “defense-in-depth” strategy by penetrating their networks to estimate and expose vulnerabilities.

Reasons why organizations recruit ethical hackers

- To prevent hackers from gaining access to the organization’s information systems
- To uncover vulnerabilities in systems and explore their potential as a risk
- To analyze and strengthen an organization’s security posture, including policies, network protection infrastructure, and end-user practices
- To provide adequate preventive measures in order to avoid security breaches
- To help safeguard the customer data
- To enhance security awareness at all levels in a business

4.9.5 Scope and Limitations of Ethical Hacking

Security experts broadly categorize computer crimes into two categories: crimes facilitated by a computer and those in which the computer is the target. Ethical hacking is a structured and organized security assessment, usually as part of a penetration test or security audit, and is a crucial component of risk assessment, auditing, counter fraud, and information systems security best practices. It is used to identify risks and highlight remedial actions.

It is also used to reduce Information and Communications Technology (ICT) costs by resolving vulnerabilities.

Ethical hackers determine the scope of the security assessment according to the client’s security concerns. Many ethical hackers are members of a “Tiger Team.” A tiger team works together to perform a full-scale test covering all aspects of the network, as well as physical and system intrusion.

An ethical hacker should know the penalties of unauthorized hacking into a system. No ethical hacking activities associated with a network-penetration test or security audit should begin before receiving a signed legal document giving the ethical hacker express permission to perform the hacking activities from the target organization.

Ethical hackers must be judicious with their hacking skills and recognize the consequences of misusing those skills.

The ethical hacker must follow certain rules to fulfill their ethical and moral obligations. They must do the following:

- Gain authorization from the client and have a signed contract giving the tester permission to perform the test.
- Maintain confidentiality when performing the test and follow a Nondisclosure Agreement (NDA) with the client for the confidential information disclosed during the test. The information gathered might contain sensitive information, and the ethical hacker must not disclose any information about the test or the confidential company data to a third party.
- Perform the test up to but not beyond the agreed-upon limits. For example, ethical hackers should perform DoS attacks only if they have previously agreed upon this with the client. Loss of revenue, goodwill, and worse consequences could befall an organization whose servers or applications are unavailable to customers because of the testing.

The following steps provide a framework for performing a security audit of an organization, which will help in ensuring that the test is organized, efficient, and ethical:

- Talk to the client and discuss the needs to be addressed during the testing
- Prepare and sign NDA documents with the client
- Organize an ethical hacking team and prepare the schedule for testing
- Conduct the test
- Analyze the results of the testing and prepare a report
- Present the report findings to the client

However, there are limitations too. Unless the businesses first know what, they are looking for and why they are hiring an outside vendor to hack their systems in the first place, chances are there would not be much to gain from experience. An ethical hacker, thus, can only help the organization to better understand its security system. It is up to the organization to place the right safeguards on the network.

SUMMARY

Digital forensics, a key facet of cybersecurity, involves investigating digital evidence and cybercrimes across various devices. Initially limited to computer forensics, it now spans all digital data storage devices, becoming indispensable for law enforcement and businesses in an increasingly digital world. Digital forensics entails identifying, preserving, examining, and analyzing digital evidence with scientific rigor. It encompasses five branches focusing on seizing, imaging, and analyzing digital media. Its primary role is supporting or refuting hypotheses in criminal and civil cases. Digital forensics is pivotal in uncovering data breaches, cyberattacks, and data leaks, as well as in incident response for recovering lost or stolen sensitive data.





REFERENCES

- 1 https://mrcet.com/downloads/digital_notes/CSE/III%20Year/12082022/DIGITAL%20FORENSICS.pdf
- 2 [https://uou.ac.in/sites/default/files/slm/MIT\(CS\)-202.pdf](https://uou.ac.in/sites/default/files/slm/MIT(CS)-202.pdf)
- 3 <https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools>

CHAPTER 5

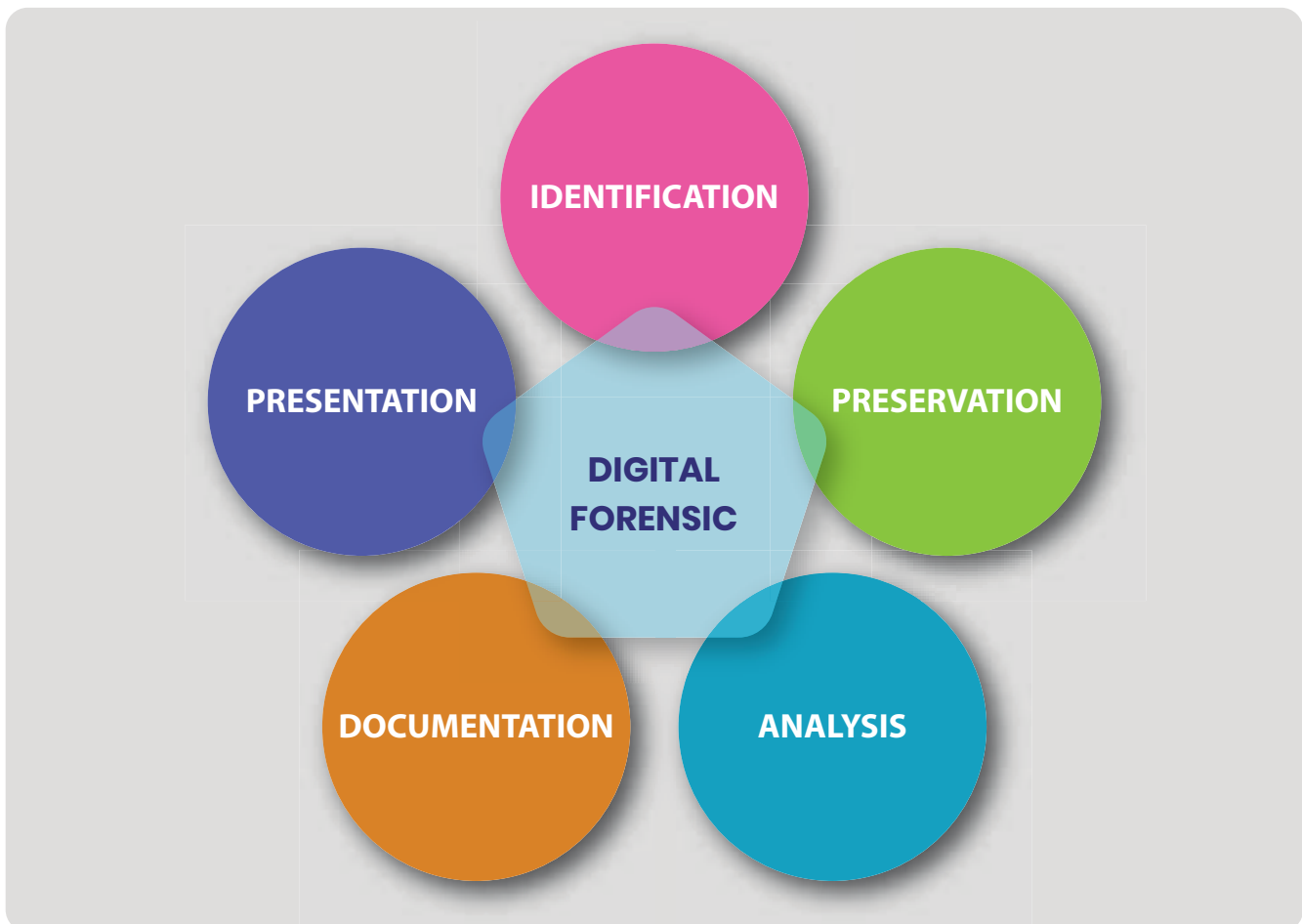
DIGITAL FORENSIC PROCESS



LEARNING OBJECTIVES

- Understanding Process of digital forensics
- Understanding stages in digital forensic process
- Understanding case study of the process

5.1 DIGITAL FORENSIC PROCESS



Digital forensic process involves the systematic and methodical investigation of digital devices, systems, and networks to gather and analyze digital evidence for legal purposes. It typically follows a structured approach to ensure the integrity and admissibility of evidence in court. The process can be broken down into several stages:

5.1.1 IDENTIFICATION

The identification phase is the starting point of the digital forensic process. It helps the person conducting the investigation to get ready and plan the steps. Here's what happens in simpler terms:

- **Case Intake:** This is where the person doing the investigation learns about the case. They find out who is involved, what happened, what kind of evidence they need, and what the legal consequences might be.
- **Case Assessment:** The investigator tries to understand the case fully. They figure out which digital devices might have important evidence, and how important that evidence might be. They also decide what skills and tools they need for the investigation.
- **Objective Definition:** The investigator decides what they want to find out from the investigation. These are the specific questions they want to answer. They make sure these objectives align with what the law requires and what the investigation is expected to achieve.
- **Legal and Ethical Considerations:** The investigator makes sure they follow all the laws and regulations that apply to collecting and analyzing digital evidence. They also respect the rights of the people involved in the case.
- **Resource Allocation:** The investigator figures out what resources they need for the investigation, like staff, tools, and equipment.
- **Risk Assessment:** The investigator looks at the things that might go wrong during the investigation and plans for those problems.
- **Scope Definition:** The investigator decides what digital devices and data sources to check, and what specific areas to focus on.
- **Initial Documentation:** The investigator keeps detailed records of everything they do and decide during the identification phase. This helps keep everything transparent and accountable.

5.1.2 PRESERVATION

The preservation of digital evidence (DE) presents unique problems beyond traditional evidence preservation. Digital evidence includes any information in binary form that can be useful in criminal or other legal investigations and proceedings. By its nature, digital evidence resides on physical media, but it is the content and related information, rather than the media, that are most often important.

Digital storage can contain an exceptionally large amount of information in a small physical footprint. It is present in a growing number of cases, owing to the ubiquitous presence of cell phones, social media use, and the vast array of digital helpers often called the Internet of Things (IoT). Digital data can be easy to change but there are powerful techniques for preventing and detecting change.

5.1.3 ANALYSIS

The analysis phase involves using collected data to prove or disprove a case built by the examiners. Here are key questions examiners need to answer for all relevant data items:

- Who created the data
- Who edited the data
- How the data was created
- When these activities occur

In addition to supplying the above information, examiners also determine how the information relates to the case.

The analysis phase in the digital forensic process is crucial. Here, the gathered digital evidence is examined to not only understand what happened but also how it happened. It involves complex and detailed techniques to uncover data, including hidden, deleted, or encrypted data. The steps typically include:

- **Data Recovery:** Extracting data from the digital device. This can involve recovering deleted files or accessing encrypted data.
- **Examination:** The data is then examined. This often involves looking for specific files or types of files, examining data in detail, and looking for evidence of particular activities.
- **Analysis:** The data is analyzed to draw conclusions about the digital behavior of the suspect. This could be identifying patterns of behavior, determining when certain files were created or accessed, or identifying the source or destination of emails or other communications.
- **Reporting:** The findings are then written up into a formal report, detailing the steps taken, the evidence found, and the conclusions drawn. This may be used in a court of law or for other official purposes.

Note that the analysis phase must be carried out in a forensically sound manner to ensure that the results are reliable and admissible in a court of law. This means that the data must be handled carefully to avoid alteration, contamination or loss, and the process should be documented thoroughly and accurately.



5.1.4 DOCUMENTATION

The documentation process in digital forensic investigations is very important, as it permanently records all relevant information generated during the investigation. This recorded data assists decision-makers, legal authorities, and administrative bodies in their respective decision-making processes. Forensic investigation professionals dedicate a significant amount of time, between 50%-75%, to writing administrative and research reports.

Documentation is a continuous process that spans the entire investigation. It meticulously records the location and status of computers, storage media, and other electronic devices. While there are overlaps between digital and physical forensic investigations, the process of documentation is crucial in both.

Computers are often involved in criminal investigations. For instance, through a search warrant, the email and internet activities of murder and rape suspects may be analyzed to gather evidence about motives or hiding locations. In the corporate world, computers are investigated when an employee is suspected of unauthorized actions. Fraud investigations often involve collecting transaction history evidence from servers. Nonetheless, it's crucial to recognize the unique differences in the implementation of the documentation process within digital and physical investigations.

5.1.5 PRESENTATION/REPORTING

To present the evidence in a way the court deems admissible and bring the guilty to justice, formulating a coherent and comprehensive digital **forensics report** is crucial. Without one, retelling the events that occurred in a structured manner, all while backing up every claim with concrete evidence, would be next to impossible (hence they are a requirement in the court proceedings).

Digital forensics reports play an instrumental role in coordinating the work between multiple investigators, law enforcement officers, administrative, and legal personnel involved in the case, not all of which may share the same professional background and field of expertise.

They are the interdisciplinary focal point that tells the truth of what happened and documents the findings, all while presenting them in a factual yet understandable manner.

At the same time, investigators should keep in mind that other law enforcement institutions may ask for the report in order to:

- STEP 1: Familiarize yourself with the best practices of writing a digital forensic report
- STEP 2: Study some generic and recommended forensic report examples before writing
- STEP 3: Write the digital forensics report
- STEP 4: Re-check your report for factual correctness and apply edits as needed
- STEP 5: Present the report to the court

Digital Forensic Lab can help you automate your reporting conclusion.

5.2 DIGITAL FORENSIC INVESTIGATION PROCESS:

The digital forensic process is a series of steps taken to uncover and interpret electronic data. The goal is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information for the purpose of reconstructing past events.

Here, it is divided into two parts according to the location of investigation.

At Crime Scene Investigation

- 1 Identification**
- 2 Collection**
- 3 Preservation**

In Lab Investigation

- 4 Examination**
- 5 Analysis**
- 6 Report**

1 Identification

In this stage, potential sources of relevant proof and data (devices) likewise as key custodians and sites of knowledge are known. Determine the scope of the incident Assess the case, Nature of case: internal, civil or criminal Characteristics of case.

2 Collection

Collecting digital data that will be relevant to the investigation. Collection could involve removing the electronic device(s) from the crime or incident scene so taking photos, imaging, repeating or printing out its content.

Chain of Custody (CoC)

The Chain of Custody may be a written or electronic document within which the acquisition, custody and transfers of any piece of proof square measure recorded. It should embrace all basic data relating to.

Acquisition: who, when, wherever and the way. Who noninheritable the proof, once and wherever the proof was noninheritable, and what methodology was used.

Custody: who, where however and the way long. Who had possession of the proof, wherever it absolutely was unbroken, what methodology was accustomed store it, and the way long it absolutely was unbroken.

Processing: What was done to the proof (cloning, analysis, etc.)

Transfer: Transfer of the proof from one human to a different, recorded alongside the signature of the new keeper.

Final Fate: Destruction, secure deletion of proof, come back of proof to owner, etc.

The most important thing for collecting evidence:

- 1 Documents
- 2 Lawfully capture evidence
- 3 Make cryptographically verifiable copies
- 4 Setup secure storage of collected evidence
- 5 Establish chain of custody
- 6 Analyze copies only
- 7 Use legally obtained, reputable tools
- 8 Document every step

Handling of Evidence

Digital proof is volatile and fragile and also the improper handling of this proof will alter it. Attributable to its volatility and fragility, protocols have to be compelled to be followed to confirm that information isn't changed throughout its handling.

(i.e., throughout its access, collection, packaging, transfer, and storage).

These protocols delineate the steps to be followed once handling digital proof. There are square measure protocols for the collection volatile proof. Volatile proof ought to be collected supported the order of volatility; that's, the foremost volatile proof ought to be collected initial, and also the least volatile ought to be collected last.

Order of volatile data from most to least volatile for standard systems.

- 1 Registers, cache
- 2 Routing table, [address resolution protocol or ARP] cache, process table, kernel statistics, memory
- 3 Temporary file systems
- 4 Disk
- 5 Remote logging and monitoring data that is relevant to the system in question
- 6 Physical configuration, network topology
- 7 Archival media



Evidence Handling Procedure

When handling proof throughout associate investigation, you may typically adhere to the subsequent procedures:

The most important thing for collecting evidence:

- If examining the contents of a tough drive presently placed at intervals a pc, record data regarding the pc system beneath examination.
- Take digital images of the first system and/or media that's being duplicated.
- Fill out associate in nursing proof tag for the first media or for the rhetorical duplication (whichever drive you may keep as best proof and store in your proof safe).
- Label all media fitly with associate in nursing proof label.
- Store the simplest proof copy of the proof media in your proof safe.
- A proof keeper enters a record of the simplest proof into the proof log. for every piece of best proof, there'll be a corresponding entry within the proof log.
- All examinations square measure performed on a rhetorical copy of the simplest proof, referred to as an operating copy.

A proof keeper ensures that backup copies of the simplest proof square measure are created. The proof keeper can produce tape backups once the PI for the case states that the info cannot be required in associate in nursing prompt manner.

A proof keeper ensures that each one disposition dates square measure met. The dates of proof disposition square measure assigned by the Investigator.

A proof keeper performs a monthly audit to confirm all of the simplest proof is gifted, properly held on, and labelled.

3 Preservation

The preservation of digital evidence (DE) presents unique problems beyond traditional evidence preservation. This document addresses considerations related to the preservation of digital evidence. This document is part of a series on evidence management and its primary audience is evidence management professionals. The document discusses traditional sources of digital evidence including physical storage media and digital objects and also addresses law enforcement generated digital evidence.

Preservation of Digital Evidence is the crux of Digital Forensics. As such, it must be handled in a way to ensure that it is promptly identified, preserved, collected, examined, analyzed and documented appropriately so that it is evidently weighty, authentic, reliable, believable, complete and that it passes the test of legal admissibility.

Top 10 Critical Steps in Preserving Digital Evidence

In this section, we will be discussing the critical steps that need to be followed to prevent loss of data before bringing to the forensic experts. Time is highly important in preserving digital evidence.

- 1 **Do not change the current state of the device:** If the device is OFF, it must be kept OFF and if the device is ON, it must be kept ON. Call a forensics expert before doing anything.
- 2 **Power down the device:** In the case of mobile phones, if it is not charged, do not charge it. In case the mobile phone is ON power it down to prevent any data wiping or data overwriting due to automatic booting.
- 3 **Do not leave the device in an open area or unsecured place:** Ensure that the device is not left unattended in an open area or unsecured area. You need to document things like- where the device is, who has access to the device, and when it is moved.
- 4 **Do not plug any external storage media in the device:** Memory cards, USB thumb drives, or any other storage media that you might have, should not be plugged into the device.
- 5 **Do not copy anything to or from the device:** Copying anything to or from the device will cause changes in the slack space of the memory.
- 6 **Take a picture of the piece of evidence:** Ensure to take the picture of the evidence from all sides. If it is a mobile phone, capture pictures from all the sides, to ensure the device has not tampered till the time forensic experts arrive.
- 7 **Make sure you know the PIN/ Password Pattern of the device:** It is very important for you to know the login credentials of the device and share it with the forensic experts, for them to carry out their job seamlessly.
- 8 **Do not open anything like pictures, applications, or files on the device:** Opening any application, file, or picture on the device may cause losing the data or memory being overwritten.
- 9 **Do not trust anyone without forensics training:** Only a certified Forensics expert should be allowed to investigate or view the files on the original device. Untrained Persons may cause the deletion of data or the corruption of important information.
- 10 **Make sure you do not Shut down the computer, if required Hibernate it:** Since the digital evidence can be extracted from both the disk drives and the volatile memory. Hibernation mode will preserve the contents of the volatile memory until the next system boots.

4 Examination

The purpose of the examination method is to extract and analyze digital Evidence. Extraction refers to the recovery of knowledge from its media. Before addressing the info, it's imperative to understand styles of knowledge. An in-depth systematic search of proof with reference to the incident being investigated. The outputs of examination square measure knowledge objects found within the collected information; this might embrace system- and user-generated files.

Extraction refers to the recovery of data from the media. Analysis refers to the interpretation of the recovered data and placement of it in a logical and useful format (e.g., how did it get there, where did it come from, and what does it mean?). The concepts offered are intended to assist the examiner in developing procedures and structuring the examination of the digital evidence. These concepts are not intended to be all-inclusive and recognize that not all of the following techniques may be used in a case. It is up to the discretion of the examiner to select the appropriate approach.

5 Analysis:

Analyzing a digital forensic evidence report can be a meticulous process because it involves understanding the details and technical language used in the report. Here are some steps to:

- 1 **Understand the Scope:** The report should clearly define the scope of the investigation. This includes the devices or systems that were analyzed, the nature of the suspected activity, and the timeframe of interest.
- 2 **Review the Methodology:** The report should detail the procedures used to collect and analyze digital evidence. This could involve techniques like file carving, keyword searching, timeline analysis, network forensics, etc. Make sure the methods used are appropriate for the type of investigation.
- 3 **Examine the Findings:** This is the core of the report. The findings section should provide a detailed account of the evidence discovered and how it relates to the case. This could be anything from suspicious files to damning emails or chat logs.
- 4 **Check the Conclusions:** The conclusions should logically follow from the findings. They should clearly answer the questions posed by the scope of the investigation.
- 5 **Evaluate the Documentation:** Good digital forensic reports will include thorough documentation. This could include logs of the forensic tools used, timestamps of when activities were performed, and even photos or screenshots.
- 6 **Verify the Chain of Custody:** The report should clearly document the chain of custody for the digital evidence. This is crucial for ensuring the evidence is admissible in court.
- 7 **Consider Expert Assistance:** If you're not familiar with digital forensics, it might be helpful to consult with an expert. They can provide valuable insight and help you understand the technical details of the report.

Remember, each report is unique, so the analysis will depend on the specifics of the case and the type of digital evidence involved.

6 Presentation/Reporting:

Begins with reports supporting verified techniques and methodologies. It also includes the fact that alternative competent rhetorical examiners ought to be able to duplicate and reproduce a similar result. Reporting is that the method of making ready a close outline of all the steps taken. Associate in nursing conclusions reached as a part of an examination. News ought to embrace details regarding all the vital actions performed by you, the results of the acquisition, and any inferences drawn from the results.

In general, a report may contain the following details:

- Details of the reporting agency
- Case identifier
- Forensic investigator
- Identity of the submitter
- Date of evidence receipt
- Details of the device seized for examination including serial number, make, and model.
- Details of the equipment and tools used in the examination
- Description of steps taken during examination
- Chain of custody documentation
- Details of findings or issues identified
- Evidence recovered during the examination, ranging from chat messages, browser history, and call logs to deleted messages, and so on
- Any images captured during the examination
- Examination and analysis information
- Report conclusion

SUMMARY

The digital forensic process is a systematic approach to investigating digital devices, systems, and networks for legal purposes. It involves several key stages. The Identification phase sets the groundwork for planning, involving case intake, assessment, objective definition, legal considerations, resource allocation, risk assessment, and scope definition. Preservation is critical for safeguarding digital evidence, encompassing the identification, collection, and storage of evidence in a forensically sound manner. The Analysis phase delves into the collected data to understand the 'what' and 'how' of the incident, involving data recovery, examination, and in-depth analysis while ensuring forensically sound practices. Documentation is vital for transparency, recording all pertinent information throughout the investigation.



The Presentation/Reporting phase is pivotal for presenting evidence in court, creating comprehensive reports that serve as interdisciplinary focal points. Lastly, the Digital Forensic Investigation Process spans stages conducted at the crime scene and in the lab, encompassing Identification, Collection, Preservation (at the crime scene), and Examination, Analysis, and Reporting (in the lab). Proper evidence handling is emphasized, from maintaining the device's state to ensuring chain of custody. Overall, these stages ensure a structured, accountable, and legally admissible approach to digital investigations.



REFERENCES

- 1 https://dfrws.org/wp-content/uploads/2019/06/2004_USA_paper-the_enhanced_digital_investigation_process_model.pdf
- 2 <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf>
- 3 <https://www.iasj.net/iasj/download/6e2dd4cac5720eb3>
- 4 *Unboxing the digital forensic investigation process - ScienceDirect*
- 5 (PDF) *Digital Forensics (researchgate.net)*

CHAPTER 6

INFORMATION TECHNOLOGY CRIMES AND ITS LEGAL CONSEQUENCES



LEARNING OBJECTIVES

- Understanding of IT crimes
- Types of IT crimes
- Prevention of IT crimes
- Understanding IT acts
- Understanding its legal consequences

6.1 INTRODUCTION

As the clock of progress ticks on, Information Technology (IT) stands as the harbinger of change across all spheres of life. Yet, this technological marvel has unwittingly sired a new adversary – Information Technology crimes, colloquially dubbed cybercrimes. This extensive exposé embarks on a journey through the intricate labyrinth of IT crimes, uncovering their myriad facets and entwining legal ramifications. This paper's mission is to empower individuals, conglomerates, and policymakers alike with insights to navigate this digital terrain adeptly.

6.2 TYPES OF INFORMATION TECHNOLOGY CRIMES

Within the digital underworld, a pantheon of malevolent actions thrives. Hacking and unauthorized access thrust individuals into the virtual sanctums of others. Malware attacks conjure digital pestilences, orchestrating chaos. Identity theft and phishing artfully manipulate victims into divulging confidential data. Online fraud orchestrates an intricate dance of deceit, while cyberbullying and harassment inflict psychic wounds. Intellectual property theft plunders the realm of innovation.

6.3 REAL-WORLD EXAMPLES

The annals of cyber history are replete with instances that underscore the dynamic interplay between technology and criminal intent. From grand-scale breaches that exposed vulnerabilities in security infrastructure to cleverly orchestrated social engineering ploys, each example serves as a stark reminder of the potential repercussions of the digital age.

1 Equifax Breach: Unveiling Vulnerability at Scale

In the digital age, data is power, and the Equifax breach demonstrated the devastating consequences of data falling into the wrong hands. In 2017, the credit reporting agency Equifax suffered a massive cyberattack that exposed the sensitive personal information of nearly 147 million individuals. This breach not only compromised names, social security numbers, and addresses but also highlighted the potential for widespread identity theft. The breach's magnitude and its far-reaching consequences underscored the dire need for stringent cybersecurity measures in organizations that handle sensitive data.

2 WannaCry Ransomware: A Global Digital Hostage Crisis

The WannaCry ransomware attack, which unfolded in 2017, encapsulated the borderless threat posed by cybercriminals. This malicious software rapidly spread across the globe, infecting computer systems in over 150 countries. By encrypting files and demanding a ransom in cryptocurrency, the perpetrators brought many critical systems to a standstill, affecting everything from hospitals to transportation networks. This attack was a stark illustration of the potential real-world impact of cybercrimes, transcending geographical and sectoral boundaries.

3 Nigerian Prince Scam: Exploiting Human Trust

In the realm of cybercrimes, human vulnerability is often exploited just as effectively as technological weaknesses. The infamous "Nigerian Prince" scam, although seemingly straightforward, continues to ensnare unsuspecting victims. This social engineering ploy typically involves an email from someone claiming to be royalty, requesting financial assistance or promising substantial rewards in return. Despite its apparent implausibility, the scam has duped individuals into parting with their money. The persistent success of such schemes underscores the importance of cybersecurity education and raising awareness about these tactics.

4 The Rise and Fall of Silk Road: Unveiling the Dark Web Underbelly

The Silk Road saga stands as a testament to the depth and complexity of cybercrime networks. Operating on the Dark Web, the Silk Road was an online marketplace notorious for facilitating illegal transactions, primarily involving drugs and other contraband. Through advanced encryption and cryptocurrency transactions, the Silk Road enabled users to carry out illegal exchanges anonymously. Its eventual takedown by law enforcement demonstrated the concerted effort required to combat cybercrime in its most hidden and encrypted corners.

6.4 LEGAL FRAMEWORK FOR IT CRIMES IN INDIA

In the quest to combat Information Technology (IT) crimes, legal frameworks in India have emerged as the frontline defenses against the ever-evolving landscape of cyber threats. While global efforts like the Budapest Convention endeavor to harmonize cybercrime legislation, India's own legal apparatus has been fortified to address the unique challenges posed by IT-related transgressions. These legal instruments not only define cybercrimes but also outline the punitive measures and procedures for prosecution, echoing the nation's commitment to secure its digital realm

6.5 THE INFORMATION TECHNOLOGY ACT, 2000

Central to India's response to cybercrimes is the Information Technology Act, 2000 (IT Act). This landmark legislation was formulated to provide legal recognition to electronic transactions, facilitate e-governance, and establish a robust legal framework to address cybercrimes. Under

this act, various offenses related to hacking, data theft, unauthorized access, and damage to computer systems are defined. The act also introduced the concept of digital signatures and electronic records, bolstering the credibility of electronic transactions.

6.6 AMENDMENTS AND STRENGTHENING

Recognizing the rapid evolution of technology and the consequent emergence of new cyber threats, the IT Act underwent significant amendments in 2008. These amendments broadened the scope of cybercrimes, introducing provisions to penalize offenses like cyberterrorism, child pornography, and identity theft. The amendment also introduced intermediary liability, establishing the responsibilities of online platforms and service providers to prevent the proliferation of illicit content.

6.7 CYBER APPELLATE TRIBUNAL

To ensure swift and effective adjudication of cybercrimes, the IT Act established the Cyber Appellate Tribunal (now subsumed under the Telecom Disputes Settlement and Appellate Tribunal). This specialized judicial body was designated to hear appeals against orders issued by the Controller of Certifying Authorities and the Adjudicating Officer appointed under the IT Act. The tribunal played a pivotal role in addressing legal challenges arising from cyber incidents, ensuring a focused and informed approach to cybercrime cases.

6.8 PUNITIVE MEASURES AND DUE PROCESS

The IT Act stipulates a range of punitive measures for various cyber offenses. These penalties include imprisonment and fines, with severity varying based on the nature and gravity of the crime. The legal process outlined in the act ensures due process, requiring the prosecution to prove the accused's guilt beyond a reasonable doubt.

6.9 CROSS-BORDER CHALLENGES

While India's legal framework is robust within its jurisdiction, traversing international legal terrains in cases involving cross-border cybercrimes remains intricate. Challenges arise when offenders operate from jurisdictions with differing legal standards, making extradition and cooperation with foreign authorities' complex endeavors. The extraterritorial nature of cybercrimes necessitates a delicate balance between enforcing Indian laws and respecting international legal norms.

6.10 LEGAL CONSEQUENCES OF IT CRIMES

Stepping into the realm of legal consequences within the sphere of Information Technology, crimes unveils a labyrinthine landscape, where the punitive aftermath mirrors the diverse forms of transgressions committed. The judicial response to these offenses ranges across a spectrum as broad as the crimes themselves, reflecting the complexity of modern digital malfeasance.

Criminal penalties, the traditional domain of legal retribution, demonstrate a wide variance in

severity. Monetary fines, often calibrated based on the financial harm inflicted, strive to equate the loss with a tangible price. Yet, as the gravity of the crimes escalates, so do the penalties. The digital marauder, who breaches the sanctum of another's digital domain, might find themselves sentenced to a term of imprisonment. Strikingly, some jurisdictions don't shy away from imposing life sentences for cybercrimes of unprecedented magnitude, underscoring the magnitude of the harm that can be wrought within a few lines of malicious code.

Parallel to criminal justice, civil remedies introduce a dimension of restoration for the aggrieved. Victims grappling with the aftermath of digital pillaging are afforded avenues to reclaim their lost ground. Courts may decree restitution to victims, aiming to resurrect what was filched from them in the digital heist. This duality of punitive and reparative aspects showcases the multifaceted nature of legal consequences in the virtual arena.

However, as digital space transcends geographical borders, the intricacies of extradition and jurisdiction unveil a conundrum. The elusive nature of cybercriminals, who often operate anonymously across international boundaries, presents challenges in delivering justice. Extradition, the process of surrendering the accused from one jurisdiction to another, becomes a delicate dance where legal intricacies and diplomatic protocols intermingle. Additionally, the diverse legal standards across nations can lead to ambiguity in pinpointing the appropriate jurisdiction to conduct proceedings.

In this digital frontier, where codes traverse borders without pause, the notion of jurisdiction itself is muddled. The digital culprits, unfettered by physical constraints, can seamlessly orchestrate transgressions across a multitude of domains. This evasive quality blurs the lines of jurisdictional control, leaving legal systems grappling with the question of where the long arm of the law should reach.



6.11 INVESTIGATING AND PROSECUTING IT CRIMES

Unveiling cybercriminal plots mandates specialized acumen. Digital forensics meticulously traces breadcrumbs across digital domains. Law enforcement agencies convene with cybersecurity savants to apprehend wrongdoers. Amid this, questions of due process and digital liberties emerge.

Mitigating IT Crime Risks:

Mitigating IT Crime Risks: A Multi-Faceted Strategy

As the digital landscape expands and cyber threats become increasingly sophisticated, the imperative to preempt Information Technology (IT) crimes has never been more pressing. The battle against cyber malevolence demands a comprehensive, multi-pronged approach that draws from a spectrum of strategies, each intricately designed to fortify the digital realm against the relentless tide of cyber threats.

6.12 CYBER SECURITY DOCTRINES: BUILDING A FORTIFIED DIGITAL BASTION

At the core of IT crime mitigation lies the implementation of robust cybersecurity doctrines. These doctrines encompass an array of measures aimed at safeguarding digital assets and sensitive information. Consistent software updates, often overlooked but critically important, plug vulnerabilities that cybercriminals are quick to exploit. Coupled with this is the rigorous enforcement of impregnable encryption protocols that render intercepted data indecipherable to unauthorized entities. The collaboration between cybersecurity experts and software developers becomes a formidable alliance, working relentlessly to anticipate and thwart potential breaches.

6.13 EMPLOYEE EDUCATION: FORTIFYING THE HUMAN FIREWALL

In the realm of IT crimes, human vulnerability often proves to be a chink in the armor. This vulnerability is exploited through techniques like phishing and social manipulation, where unsuspecting individuals inadvertently become conduits for cyber-attacks. To counter this, an enlightened workforce becomes the first line of defense. Initiatives to educate employees about the subtleties of phishing attacks and the art of social engineering play a pivotal role in curtailing susceptibility. By fostering a culture of cyber vigilance and empowering employees with the knowledge to discern between legitimate and malicious communications, organizations erect a robust human firewall against IT threats.

6.14 PUBLIC-PRIVATE ALLIANCES: FORGING A UNITED FRONT

Recognizing the all-encompassing nature of cyber threats, the convergence of efforts between the public and private sectors emerges as a linchpin strategy. Public-private alliances constitute a dynamic framework where governmental bodies, law enforcement agencies, and private corporations collaborate synergistically. This collaboration yields a two-fold advantage: the sharing of threat intelligence and the pooling of resources for proactive defense.

Intelligence-sharing enables a real-time understanding of emerging threats and their modus operandi, enabling stakeholders to fortify their defenses preemptively. The synergy between the public and private sectors transcends organizational boundaries, creating a united front against the omnipresent menace of IT crimes.

6.15 TECHNOLOGICAL INNOVATION: STAYING AHEAD OF THE CURVE

In the perpetual chess game between cyber attackers and defenders, innovation becomes a crucial differentiator. Technological advancements offer an arsenal of tools that can be wielded against IT crimes. Artificial Intelligence (AI) and Machine Learning (ML) algorithms, for instance, possess the capability to detect patterns indicative of cyber threats in real-time, automating threat identification and response. Behavioral analysis tools decode deviations from normative user behavior, sounding alarms at the first signs of unauthorized access. Moreover, blockchain technology, renowned for its immutable nature, bolsters the integrity of digital transactions and data storage, deterring data tampering and fraud.

6.16 CRAFTING A RESILIENT DIGITAL FUTURE

Mitigating IT crime risks is a mission that demands comprehensive preparedness, collaborative engagement, and technological acumen. As the digital landscape evolves, so must our strategies to protect it. The multi-faceted approach – a blend of robust cybersecurity, empowered human resources, public-private collaboration, and innovative technologies – emerges as the cornerstone of a resilient digital future. This multifarious strategy, continually refined and adapted, stands as a testament to our unwavering commitment to secure the digital realm against the relentless tide of cyber threats.



6.17 CASE STUDIES: LANDMARK IT CRIME TRIALS

In history's annals, some trials become epitomes. The saga of Kevin Mitnick chronicles a hacker's odyssey through legal labyrinth. The Gary McKinnon saga epitomizes jurisdiction's challenge in cross-border cybercrime. Operation Aurora illuminates the ominous shadow of state-sponsored digital assaults.

6.18 THE EVOLVING NATURE OF IT CRIMES

As technology gallops ahead, cybercrime morphs. Artificial Intelligence becomes a menacing accomplice in the realm of wrongdoing. Ransomware as a Service democratizes extortion. The enigma of the Deep Web defies conventional investigative paradigms.

6.19 GUIDELINES GIVEN BY SEBI FOR MARKET INFRASTRUCTURE INSTITUTIONS (MIIS):

- 1 **Robust Cybersecurity Framework:** MIIs must establish and maintain a robust cybersecurity framework to safeguard the confidentiality, integrity, and availability of data and IT systems. Emphasize the importance of continuous improvement in IT processes and controls.
- 2 **Interconnectedness Awareness:** MIIs should be aware of the increased interconnectedness and interdependency among MIIs. Cybersecurity measures should extend beyond owned or controlled systems to cover all interconnections and dependencies.
- 3 **Guideline Compliance:** Ensure MIIs comply with the guidelines issued by SEBI for strengthening cybersecurity and cyber resilience. Encourage a proactive approach to implementing these guidelines.
- 4 **Compliance Reporting:** MIIs are required to provide compliance reports along with cybersecurity audit reports. Stress the importance of timely and accurate reporting in accordance with existing reporting mechanisms.
- 5 **Testing and Preparedness:** Promote regular cybersecurity practices, including offline data backups, system image maintenance, vulnerability scanning, and business continuity drills. Encourage MIIs to actively test their response and recovery plans, including scenarios involving ransomware attacks and extreme cyber incidents

6.20 FUTURE TRENDS AND CONCLUSION

As we cast our gaze toward the horizon, we behold a landscape that reverberates with the echoes of emerging technologies. Among these, quantum computing stands as a spectral enigma, casting a dual-edged shadow over the domain of cyber security. Quantum computing

possesses the potential to revolutionize encryption, both as a formidable guardian and a formidable threat. Its unprecedented computational power, harnessed through the manipulation of quantum bits or qubits, has the capacity to break existing cryptographic methods, rendering the foundations of digital security vulnerable. Simultaneously, quantum cryptography offers the promise of unbreakable codes, thereby raising the bar for cyber resilience to unprecedented heights.

However, as quantum computing presents a shifting battleground, it magnifies the significance of adaptation – a crucial imperative resonating in both the legal and technological spheres. Legal frameworks must evolve nimbly to encompass the intricate nuances of quantum threats, devising legislation that remains agile in the face of swift technological advancements. This dynamic interplay necessitates legal minds that can grapple with the complexities of cryptography, quantum physics, and cyber law in tandem.

Simultaneously, technological adaptation becomes a steadfast bulwark against the advancing tide of cybercrimes. With each innovation, cybercriminals find new avenues to exploit vulnerabilities. It is incumbent upon the cybersecurity community to remain a step ahead, developing resilient defenses that anticipate and counter these evolving threats. Furthermore, the synergy between legal and technological expertise is paramount, as laws and regulations must be enforced through robust technical implementations.

The pursuit of justice in the realm of IT crimes transcends solitary endeavors. It beckons a collaborative pact between nations, organizations, and individuals – a pact where the conventional borders of jurisdiction blur in the name of safeguarding digital justice. Global cooperation, information sharing, and mutual support are not merely admirable ideals but a practical necessity in the fight against cyber malevolence. The harmonization of legal standards, the sharing of threat intelligence, and the collective commitment to secure the digital landscape form the bedrock of this collaborative crusade.



REFERENCES

- 1 *CYBER LAW & CYBER CRIMES SIMPLIFIED* by Cyber Infomedia
- 2 *Beyond Productivity: Information, Technology, Innovation, and Creativity*
- 3 *ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary*

CHAPTER 7

DIGITAL FORENSICS TOOLS AND USAGE OF OSINT TOOLS FOR CYBER FORENSICS



LEARNING OBJECTIVES

- Understanding digital forensics tools
- Usage of OSINT TOOLS
- Understanding types of digital forensics tools
- Usage of tools for cyber forensics

7.1 INTRODUCTION

The Importance of Digital Forensics

In the contemporary digital age, digital forensics stands as a critical pillar in the realm of investigations. It encompasses the systematic collection, preservation, analysis, and presentation of digital evidence, playing an instrumental role in resolving cybercrimes, supporting legal proceedings, and ensuring the integrity of data.

Role of Tools in Modern Investigations

At the heart of modern investigations lies the utilization of digital forensics tools. These tools serve as indispensable assets that streamline the intricate process of extracting, analyzing, and interpreting digital evidence from an array of sources, including computers, smartphones, and networks. In the face of increasingly sophisticated cybercriminal activities, these tools empower investigators to unravel concealed insights and reconstruct digital events with precision.



7.2 UNDERSTANDING DIGITAL FORENSICS TOOLS

7.2.1 CATEGORIES OF DIGITAL FORENSICS TOOLS

Digital forensics tools can be classified into various categories based on their functionalities and utilities:

- **Disk and File Analysis Tools:** These tools delve into storage media, recover erased files, and scrutinize file metadata.
- **Memory Analysis Tools:** Memory forensics tools unravel the secrets of volatile memory, unveiling running processes, network connections, and potential traces of malware.
- **Network Analysis Tools:** Network forensics tools capture and analyze network traffic, shedding light on malicious activities and offering insights into network behavior.
- **Malware Analysis Tools:** These tools dissect and scrutinize malware samples, enabling analysts to fathom their behavior and impact.
- **Timeline Generation Tools:** These tools orchestrate the construction of chronological timelines, vital for unraveling the sequence of digital incidents

7.2.2 SIGNIFICANCE OF DIGITAL EVIDENCE

The very essence of modern investigations rests on digital evidence. It encompasses a vast array of data, ranging from computer files and emails to logs and digital artifacts. Digital forensics tools play a pivotal role in ensuring the accurate collection, preservation, and analysis of this evidence, rendering it admissible in legal proceedings. Maintaining the integrity and authenticity of digital evidence is of paramount importance, a role that these tools undertake with precision.

7.3 DIGITAL FORENSICS LANDSCAPE

7.3.1 THE GROWING THREAT OF CYBERCRIME

Cybercrime looms as an ever-increasing and evolving menace, presenting significant challenges to individuals, organizations, and governments alike. With cybercriminals perpetually devising new techniques and strategies, the imperative for robust digital forensics practices becomes even more pronounced. Cyber forensics experts must remain one step ahead to counteract the escalating complexity of cyberattacks.

7.3.2 EVOLUTION OF CYBER ATTACKS

The evolution of cyberattacks has transitioned from simple viruses to intricate, targeted endeavors. Attack vectors now encompass a spectrum of techniques, including malware propagation, phishing campaigns, and the deployment of ransomware. This evolution underscores the indispensability of digital forensics tools capable of adapting to the shifting methodologies of cybercriminals while discerning patterns indicative of cybercrimes.

7.4 DIGITAL FORENSICS TOOLS

1 EnCase

Guidance Software are the creators of EnCase. It is one of the widely used forensic tools in world. In fact, 90% of the consumer goods companies around the world, 93% of the banks, 100% of the federal agencies, 75% of the power distributors and 80% of the Universities in the U.S. use Encase.

Triage: EnCase Forensic gives you the capacity to rapidly view and inquiry potential confirmation to figure out if assist examination is justified.

Collect: It helps to obtain more evidence by collecting from a variety of file formats and operating systems.

Decrypt: Here, it uses Tableau Hardware for password recovery and decryption is done.

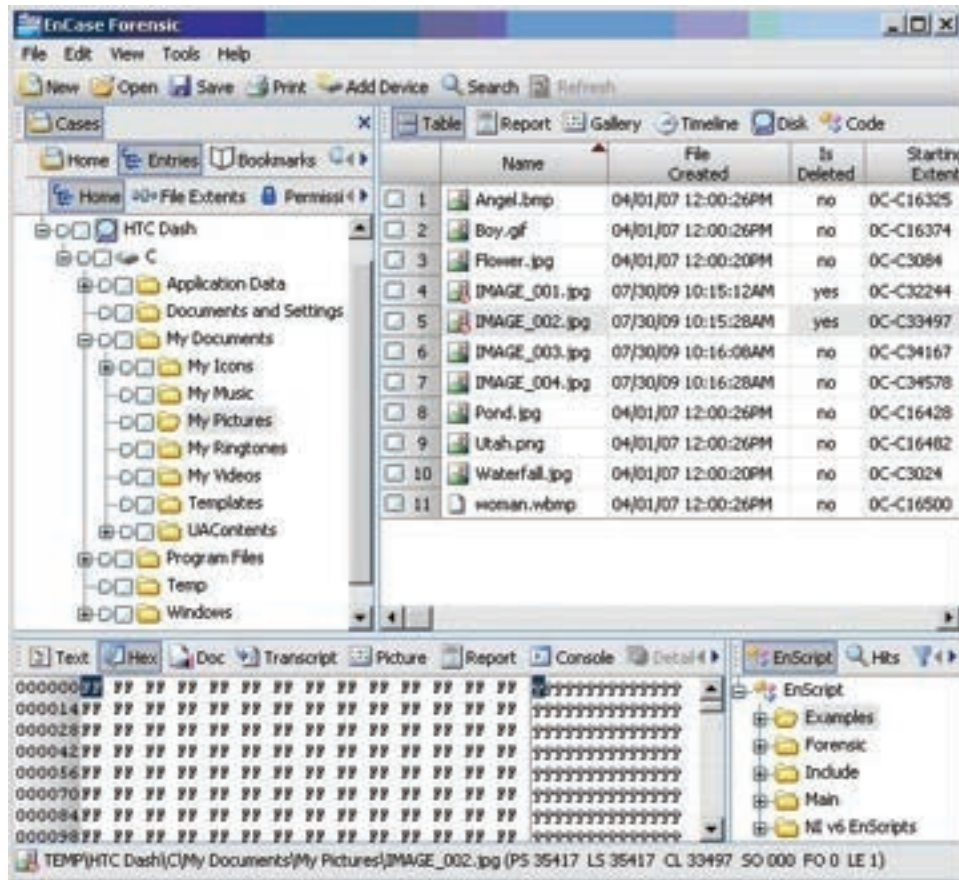
Process: As EnCase is built specifically for speed and performance which can automate complicated queries.

Investigate: The crucial part for any investigation is the ability to analyze evidence and to use the expertise to lead the way for performing investigation.

Report: EnCase provides a reporting framework which enables the investigator or user to create reports.

The following are the features of the EnCase Forensic:

- o Can gather data from vast variety of sources like network, cloud, mobile devices
- o Can produce large-scale of reports on findings while keeping the integrity of the evidence
- o It uses metadata, keywords and hash values to conduct on targeted device and collection
- o Memory acquisition
- o Can perform Disk Imaging
- o EnCase Forensic Imager can be used through USB drive and can acquire data from live device
- o Data Carving can be performed
- o Password Recovery
- o Remote data collection and processing



2 Digital Forensic Framework (DFF)

Digital Forensics Framework is an Open-Source forensics platform which is developed on a customized Application Programming Interface. Mostly used by the law enforcement agencies, educational institutions and private companies around the world. It is available in three options as DFF which is free, DFF Pro, DFF Live. DFF free will not get any professional support, report editor, automation engine, user activities reporting, hash scanner and skype analysis when compared with DFF Pro and DFF Live.

The following are the features of DFF:

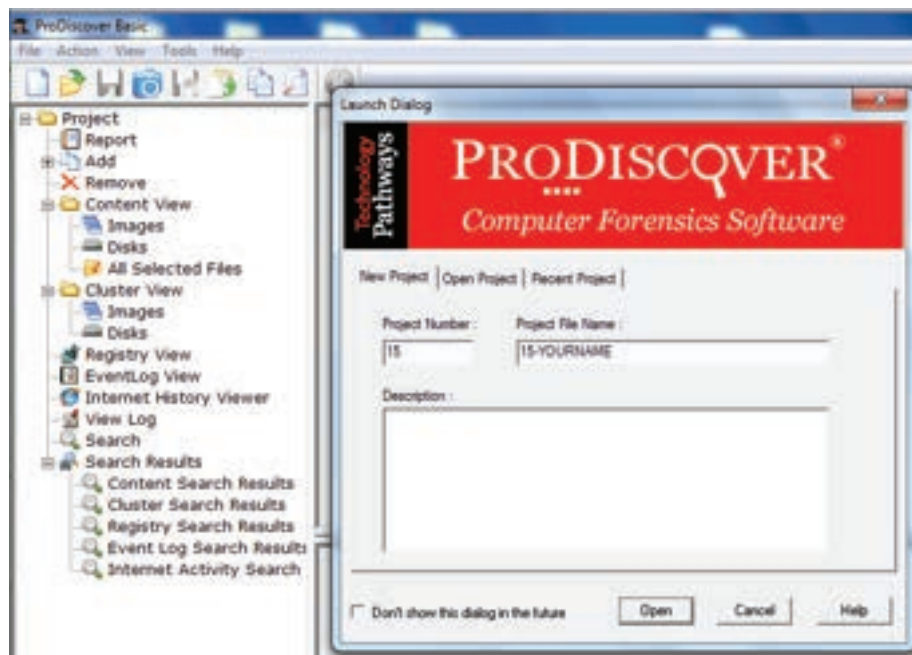
- o It can perform Cryptographic hash calculation
- o Can perform EXIF meta-data extraction
- o Can import all Microsoft Outlook mailboxes
- o Memory Dump analysis
- o Scripting and batching capabilities
- o Instinctive reporting of valuable information and web browsing
- o Can automatically extract data
- o Can perform investigation during live and static analysis

3 Pro-Discover

The ARC Group of New York are the founders of Pro Discover Forensic. It is available in three options as Pro Discover Basic for, Pro Discover Forensic Edition for and Pro Discover Incident Response Edition. The Pro Discover Basic gathers snapshots of activities which are essential for taking steps to protect user data. We can collect time zone, web browsing activities and device information through a report when required. Whereas, Pro Discover Forensic Edition allows the inspection of files without making any changes to the metadata like the last time accessed and Pro Discover Incident Response Edition is a reactive, interactive and proactive forensic investigation tool. It allows the investigators to perform live analysis. It also uses a patent pending technology and process called Connect Collect Protect which helps the user to connect to a device, gather data and analyze the situation during any security issue or data breach.

The following are the features of Pro Discover Forensic:

- o It allows inspection, image capture and search of Hardware Protected Area
- o To find the data, it uses Boolean search capability to search for regular expressions and keywords
- o It is flexible and fast
- o Pro Discover Incident Response Edition can help to stop the threat within the minutes of alert
- o One can install the SMART AGENT when required and can remove when it is done
- o It also comes with malware discovery hash sets
- o Uses Perl Scripts for performing investigation tasks
- o It creates automatic reports with the information required to be presented as evidence.

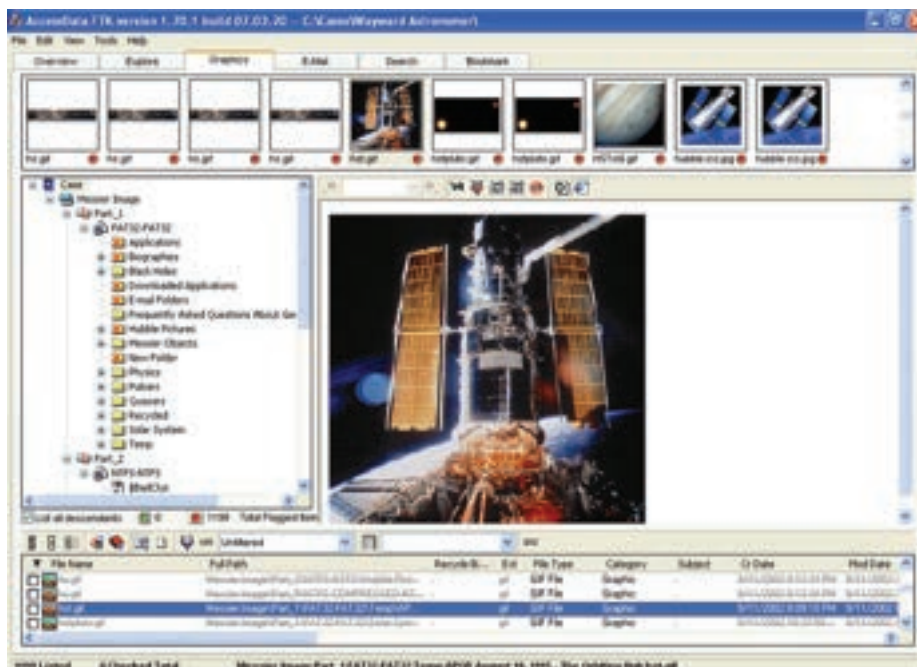


4 Forensic Toolkit (FTK)

Access Data Group are the makers of FTK. They are the major provider of forensics tool training and certification. Over 130,000 governing bodies and law firms use FTK around the world. It can perform analysis on laptops, personal computers, network communications and mobiles. Filtering and searching is faster than any other tool available.

The following are the features of FTK:

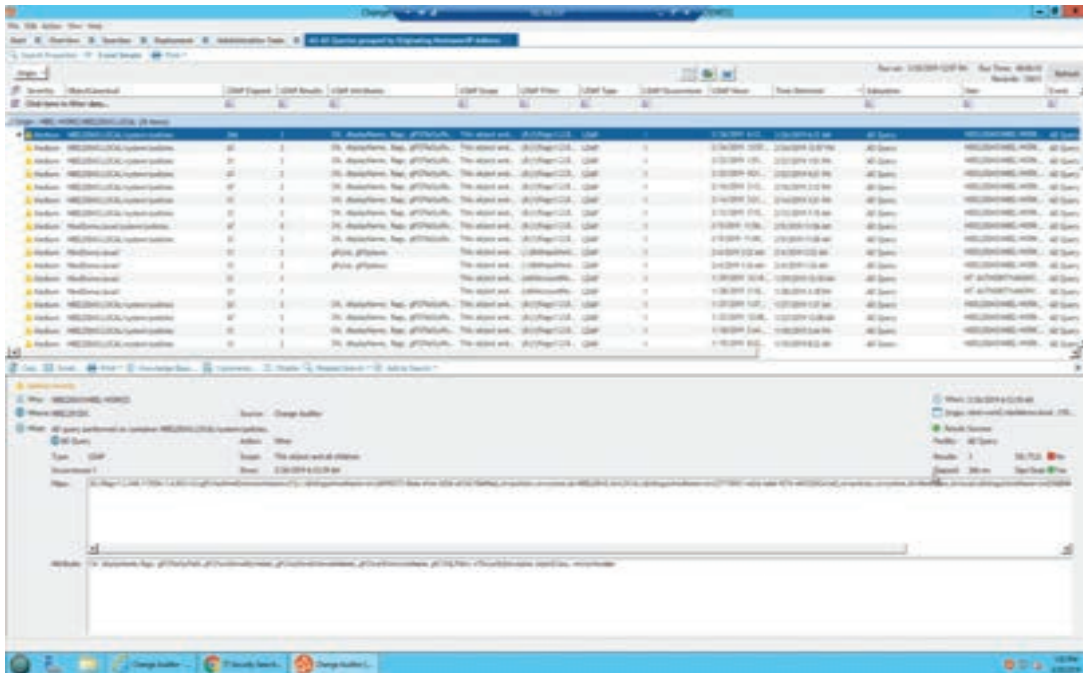
- o It can obtain and store the data across the network
- o It can acquire information from 3,500 mobile devices
- o It can easily detect missing data, spiteful behaviour and data leakage
- o If suppose, data is stored in different location from the original, FTK can identify how did it get there, who has changed the location and even identify if any changes had been done to the original.
- o It can easily identify if any data has been transferred from the system or mobile device.
- o It can even gather information during static analysis
- o One can run FTK from an USB drive
- o It has the option of expert review, where reviewing will be done and compared with the witness on the final analysis of the evidence.
- o Password recovery
- o With the help of FTK Imager, disk imaging is done
- o By using hashing techniques and Boolean, it can search data
- o By using FTK Internal viewer, the forensic officer can view Excel, PowerPoint and Word.
- o It can perform email analysis
- o It can support multi languages
- o The customer can choose pdf format or tiff format for exporting the evidence



5 Quest change auditor

The main focus of the tool is to track the real-time analysis with complete visibility. It can easily detect an insider attack and a report is generated.

- o Can check if the object has changed or not.
- o It displays the previous values and the altered values and can restore them with previous clicks.
- o Dynamic investigation paths are taken.
- o Can do full text search saving the time to check if file is changed and which.



6 The Sleuth Kit

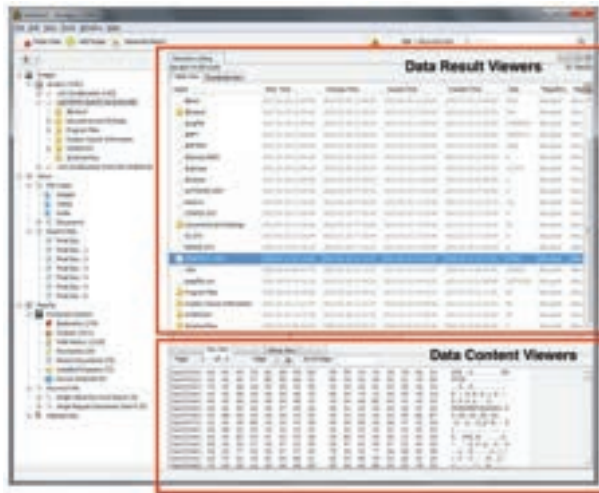
It is a library that has a collection of command line tools. Its current version is 4.3.0 which was released on July 19, 2016. The new version has support for Virtual Machine formats with the help of these libraries: libvmmdk and libvhdi. The main function of sleuth kit helps in analysing the file system data.

It helps in analysing copies of disk images of the systems under investigation and recover files from them. It is used by law enforcement bodies, military and corporate examiners perform digital forensics and come up with an explanation as to what occurred in a device. It can also be used for recovering digital media and files from the memory cards.

The framework of Sleuth Kit will supply an open platform for the operation of application layer modules. The access to the files are given by framework itself.

The Sleuth Kit's framework allows a user to easily build automated, end-to-end digital forensic applications. The framework is used for a more detailed and complex analysis of the disk image. The framework contains plug-in pipelines with which the user can incorporate many analysis techniques. If the user wants the details of only the volume level support and file system level support, then the original Sleuth Kit library can be used.

The frameworks support and was intended to be used in distributed environment so that jobs could be split among various computers. Even though that was the intention, user can also use that framework to create desktop applications.



7 Computer Online Forensic Evidence Extractor (COFEE):

COFEE was developed by Microsoft to extract evidence from Windows [18]. The forensic investigator can perform live analysis by installing COFEE on a pen drive or hard disk. Microsoft is currently working with Interpol and National White Collar Crime Center (NW3C) to perform forensic investigation. COFEE is not made available to everyone except law enforcement agencies.

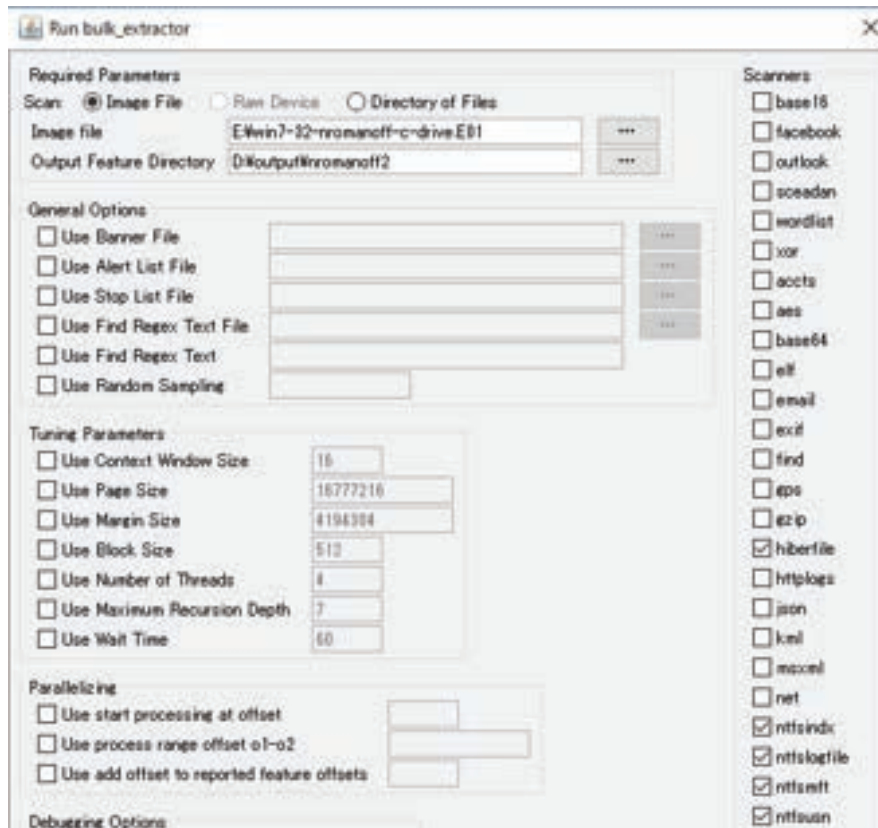


8 Bulk Extractor

The Bulk Extractor is a window, Linux and MAC based tool. The main advantage of bulk extractor is it ignores all the type of file system so, any kind of file will be supported to run on the bulk extractor.

The main features of bulk extractor are: -

- o It can perform disk imaging
- o Can Recover the data
- o Data carving is possible
- o Password can be recovered
- o It can make an analysis on email
- o Live analysis on any system can be performed
- o And can decrypt the file if it is encrypted



9 Cellebrite UFED

The UFED (Universal Forensics Extraction Device) is a product series of the Israeli company Cellebrite, which is used for the extraction and analysis of data from mobile devices by law enforcement agencies.

On the UFED Touch, it is possible to select extraction of data and choose from a wide list of vendors. After the data extraction is done, it is possible to analyze the data in the Physical Analyzer application.

The Cellebrite UFED Physical Analyzer supports the following features:

- o Extract device keys which can be used to decrypt raw disk images, as well as keychain items
- o Revealing device passwords, although this is not available for all locked devices
- o Passcode recovery attacks
- o Analysis and decoding of application data
- o Generating reports in various formats such as PDF and HTML
- o Dump the raw file system for analysing it in other applications

At a software level, Cellebrite's Physical Analyzer tool then helps clients dig through the terabytes of data often stored on consumer devices today. The company combines keyword-based filtration with artificial intelligence (AI) to surface specific information.

Finally, in order to preserve evidentiary integrity, Cellebrite's hardware is supported by a management suite that keeps a strict activity log and audit trail.

"It's critical to have transparency about who is handling evidence, because there are concerns about both privacy and tampering," said Gambill. "Our solution is able to demonstrate precisely who has accessed what data and when."

Even more than most companies, Cellebrite has a responsibility to pick and choose which clients it works with. Indeed, Gambill admits there have been instances in which its technologies have been misused, although he stressed these are extremely rare.

To shield against this eventuality, Cellebrite has designed its hardware such that it cannot be used by anyone other than active licensees. Updates rolled out every couple of weeks also mean that out-of-date Cellebrite kit is effectively useless, "unless you want to make a flower pot out of it", Gambill quipped.



10 Cellebrite Physical Analyzer

Cellebrite Physical Analyzer is the solution for recovering and examining digital data from digital devices, applications and the cloud. It provides a comprehensive set of tools to thoroughly examine data and find important evidence. The Physical Analyzer's functionalities include automated decryption, data visualisation and reporting.

With these features, digital investigators can access a wide range of applications (11,000+), devices and file formats. It is also possible to retrieve deleted data and convert data from applications and devices into a readable format using SQLite, Python scripting and Hes Highlighting. Once the data has been accessed, visual dashboards help investigators gain insight into the collected data. Potentially interesting events can be visualised on an advanced graphical timeline. There is also an option to view the found application data in its original format.

Features of Cellebrite UFED Physical Analyzer:

The following are features of Cellebrite UFED Physical Analyzer:

- o It supports physical and advanced logical acquisition (filesystem acquisition)
- o It extracts device keys required to decrypt raw disk images as well as keychain items
- o It decrypts raw disk images and keychain items
- o It reveals device passwords (not available for all locked devices)
- o It allows the examiner to open an encrypted raw disk image file with a known password
- o It supports passcode recovery attacks
- o It supports advanced analysis and decoding of extracted application data
- o The platform provides access to physical and logical data extracted in the same user interface, making analysis easier
- o It reports generation in several popular

Advanced capabilities for:

- **iOS**
 - o Bypassing simple and complex passcode while performing physical and file system extraction on selected devices running iOS 3.0 or higher including iOS 6
 - o Real-time decryption and decoding of data, applications, and keychain real-time decryption while revealing user passwords
 - o Advanced decoding of applications
- **BlackBerry**
 - o Advanced decoding of BlackBerry Messenger (BBM), emails, locations, applications and more
 - o Real-time decryption of protected content from selected BlackBerry devices running OS 4+ using a given password

- **Android**
 - o Advanced decoding of all physical extractions performed on devices running any Android versions
 - o Advanced decoding of applications and application files
- **GPS**
 - o Advanced decoding of BlackBerry Messenger (BBM), emails, locations, applications and more
 - o Real-time decryption of protected content from selected BlackBerry devices running OS 4+ using a given password

Rich set of data

Includes calendar, call logs, contacts SMS, MMS, chats, applications

Highlighted parsed content in the Hex

Highlights the exact position for each decoded content entry, enabling full tractability between the analysed data and the Hex

Python scripting

Using the Python shell, enhances the capabilities for content decoding

Plugin and chain management

Able to run Python scripts via plugins, and edit and create new decoding chains Analysis

Malware Detection

Perform on-demand searches for viruses, spyware, Trojans and other malicious payloads in files

Project Analytics

View statistics on communications and identifying relationship strengths

Timeline Graph

Visualize events over time, view distances between events and see the number of events within a defined timespan

Exporting Locations

Export selected latitudes, longitudes, and timestamps to KML reports

Exporting Emails

Export selected emails to EML format

Embedded Text Viewer

View text files including file information, content, and Hex

Advanced search

Based either on open text or specific parameters

Watch list

Ability to highlight information based on predefined list of values

Timeline

Monitor events in a single chronological view

Image carving

Powerful feature used to recover deleted image files and fragments when only remnants are available. Only applicable for physical extraction

All projects field search

Quick search within decoded data

Conversation view

View communications between sources in date and time order

Entities bookmarks

Quick reference pointer set to analysed data item and data file item

Hex viewer

Hexadecimal view of the extracted data enabling advanced search based on multiple parameters, regular expressions and more

Hex bookmarks

Define and save specific locations in Hex data

SQLite databases viewer

Viewing, searching and exporting tables and content (including deleted data) from SQLite database file Reporting

Report generator

Generate and customize reports in different formats e. g. PDF, HTML, XML and Excel Confirmation

Hash verification

Ensures the extraction decoded is the same extraction received from UFED device



11 Magnet Forensics for Federal Agencies

Magnet AXIOM is a complete digital investigation platform that allows examiners to seamlessly acquire and analyze forensic data, as well as share their findings. This webinar will help you learn more about this new solution with an overview of the capabilities and features of AXIOM – the evolution of Magnet IEF.

Magnet AXIOM Cyber simplifies corporate investigations. Organizations of all sizes fall victim to cybersecurity threats every day. With an artifacts-first approach and built-in remote collection, Magnet AXIOM Cyber helps you quickly understand what happened so you can investigate security events quickly. Magnet Forensics Founder and CTO, and our Forensics Consultant, Jamie McQuaid, as they explore the components of AXIOM including:

AXIOM Process

- o Acquire images and analyze evidence from smartphones, computers, and more. Use Single Stage Processing to automatically acquire and prepare data for
- o examination, saving you time and helping you get to your analysis sooner.

AXIOM Examine

- o Access file system, registry, and artifact data for an in-depth, integrated analysis using active links, multiple views, filters, searches, and more.
- o Share findings quickly and easily with customizable report views.

Magnet Forensics provides innovative solutions for Enterprise, Public Safety, and Service Providers:

- o Examine digital evidence from mobile, cloud, computer, and vehicle sources, alongside third-party extractions all in one case file. Use powerful and intuitive analytical tools to automatically surface case-relevant evidence quickly.
- o Built for DFIR teams and service providers to connect all their tools, tasks, and resources into streamlined workflows to save time and get to the truth faster.
- o Magnet DVR Examiner can recover video and metadata from password protected, broken, and burnt CCTV and Surveillance DVRs in most cases, even when the data is deleted or inaccessible.
- o GrayKey can provide same-day access to the latest iOS and Android devices – often in under one hour.
- o AXIOM Cyber is a robust digital forensics and incident response solution for organizations that need to remotely acquire & analyze evidence from computers, cloud, IoT, and mobile devices.



7.5 THE POWER OF OPEN-SOURCE INTELLIGENCE (OSINT) TOOLS

7.5.1 DEFINING OSINT

Open-Source Intelligence (OSINT) involves the systematic collection and analysis of information from publicly accessible sources. OSINT tools provide investigators with the means to gather data from websites, social media platforms, public records, and a plethora of other sources. This wealth of external data contributes context and depth to investigations, enriching the traditional digital forensics arsenal.

7.5.2 OSINT IN CYBER FORENSICS

In the realm of cyber forensics, OSINT tools offer a distinctive advantage by extending the scope of data collection beyond local devices. These tools empower investigators to amass information concerning individuals, organizations, and events from a diverse array of sources. The insights garnered from OSINT bolster the investigative process, assisting in the establishment of timelines, identification of potential suspects, and corroboration of digital evidence.

7.6 INTEGRATION OF OSINT TOOLS IN TRAINING PROGRAMS

The escalating demand for adept cyber forensics professionals arises in tandem with the rising frequency and complexity of cybercrimes. OSINT tools emerge as a strategic solution to bridge the skills gap, equipping investigators with the tools and techniques required to proficiently gather and analyze external data. This augmented expertise enhances an investigator's acumen in faithfully reconstructing events and extracting meaningful insights. Benefits of OSINT Training

- **Development of Practical Skills:** OSINT training is synonymous with hands-on experience, fostering the development of practical proficiencies encompassing data collection, analysis, and visualization.
- **Contextual Comprehension:** OSINT tools broaden the context surrounding digital evidence, enabling investigators to fathom the larger narrative encompassing a case.
- **Real-World Relevance:** The practical deployment of OSINT tools mirrors real-world investigations, rendering training in these tools directly applicable and pertinent.
- **Versatility:** OSINT tools are versatile, transgressing various investigative contexts, spanning criminal investigations to cybersecurity incident response.

7.7 EXPLORING KEY OSINT TOOLS FOR CYBER FORENSICS

1 Maltego: Visualizing Data Relationships

Maltego is a strong information gathering tool for people, organizations, and their interactions. To search open data sources and point out the relationships between entities, it employs a number of transforms. It can be utilized for the following uses.

- a **Data Gathering:** Collect information from various sources.
- b **Visualization:** Create visual maps of entities and relationships.

- c Link Analysis: Identify patterns and associations in data.
- d Enrichment: Enhance data with additional details.
- e Threat Tracking: Hunt for threats and malicious actors.
- f Documentation: Organize findings and create reports.
- g Alerts: Set up monitoring for changes in entities.
- h Incident Response: Assess and respond to security incidents.
- i Collaboration: Support teamwork among investigators.
- j Evidence Presentation: Use visuals for court presentations.



2 The Harvester: Profiling Digital Identities

The Harvester is used to conduct passive information collecting by looking for emails, subdomains, hosts, and employee names connected to a target domain. It gathers information from open sources, including social media and search engines. The Harvester can be applied to digital forensics in the ways listed below:

- a Email and Contact Discovery: Find email addresses and employee names associated with a target domain.
- b Subdomain Identification: Discover subdomains to understand the scope of an investigation.
- c Host Location: Identify hosts linked to a domain, aiding in evidence location.
- d Social Media Profiling: Locate social media profiles related to the target.
- e Data Compilation: Generate a consolidated report for efficient analysis.
- f Source Verification: Cross-check and verify data from publicly available sources.

- g Evidence Collection: Identify potential digital evidence sources.
- h Digital Footprint Analysis: Build a profile of the target's online presence.

```
sampaio@kali:~$ theharvester -h
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when f
uzzing SSL sites. Check Wfuzz's documentation for more information.

.....
*
* theHarvester Ver. 3.0.6
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
.....

Usage: theharvester options

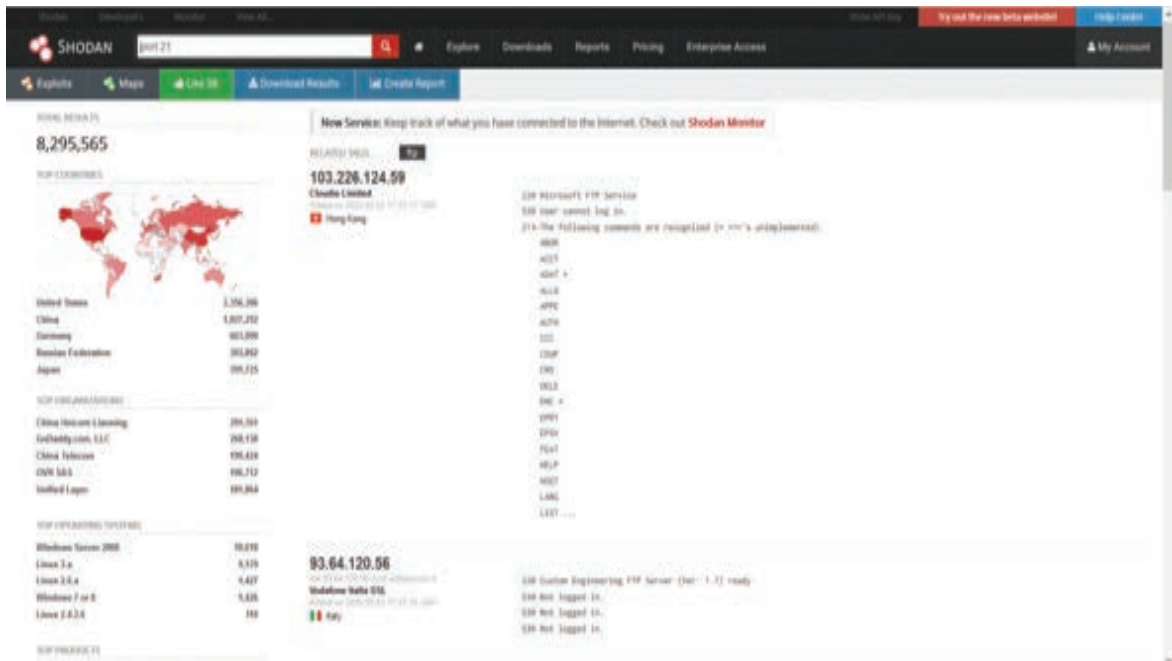
-d: Domain to search or company name
-b: data source: baidu, bing, bingapi, censys, crtsh, dogpile,
      google, google-certificates, googleCSE, googleplus, google-pro
files,
      hunter, linkedin, netcraft, pgg, threatcrowd,
      twitter, vhost, virustotal, yahoo, all
-g: use Google dorking instead of normal Google search
-s: start in result number X (default: 0)
-v: verify host name via DNS resolution and search for virtual hosts
```

3 Shodan: Uncovering Vulnerabilities

In digital forensics investigations, Shodan, a search engine for internet-connected devices, can be helpful for discovering and assessing the security of services and devices that are available via the internet. Using Shodan in digital forensics looks like this:

- a Identifying Vulnerable Devices: Shodan can help in locating internet-connected devices with open ports and services. Professionals in digital forensics might look for particular services or devices that are known to be weak points and look into possible security breaches.
- b Banner Information: Shodan gives banner information for open ports, which can provide specifics about the applications and versions being used on a device. Understanding the technology stack and any vulnerabilities may require the use of this information.
- c Network Reconnaissance: Using Shodan, investigators can perform network reconnaissance and compile data about a target's infrastructure, such as IP addresses, Domain etc.
- d Device profiling: Shodan enables users to generate profiles of internet-connected devices by gathering information about the operating system, location, and type of device. When examining a target's attack surface during digital forensics investigations, this information can be helpful.

- e Vulnerability Assessment: Shodan can be used to do initial vulnerability evaluations by detecting machines running outdated or known vulnerable software. This can help investigators decide how to prioritize their analysis tasks.
- f Historical Information: Shodan offers historical information that enables investigators to monitor changes in a device's configuration and security posture over time. This can be helpful in figuring out how a security incident developed.
- g Analysis of IoT Devices: Shodan is particularly helpful for locating and examining IoT (Internet of Things) devices, which are frequently open to abuse. The security of IoT devices connected to a network can be evaluated by investigators.
- h Alerts and monitoring: Shodan provides alerting tools that let users keep an eye out for modifications or newly discovered vulnerabilities in particular devices, services, or IP addresses. This may aid in the early identification of security problems.
- i Evidence Gathering: By discovering devices that may have been hacked or used in cyberattacks, Shodan enables investigators to locate prospective digital evidence sources.



4 Spider-Foot: Comprehensive Data Gathering

SpiderFoot is an open-source OSINT (Open Source Intelligence) application that streamlines the process of gathering data about numerous entities, including IP addresses, domain names, email addresses, and more. It can help digital forensics investigations by speeding up the data collection process. In digital forensics, SpiderFoot can be applied as follows:

- a Data collection: SpiderFoot gathers information from a variety of places, such as

search engines, open-access databases, social media sites, and WHOIS records. In the field of digital forensics, this can assist investigators in compiling important data regarding a target entity, such as a person, business, or website.

- b Entity Profiling: This feature enables investigators to profile entities by aggregating data about them. Email addresses, domain names, IP addresses, and other information are examples of this. Building a thorough awareness of the target's online presence with the use of profiling.
- c Threat Intelligence: SpiderFoot can look up indicators of compromise (IoCs) related to a target by scouring threat intelligence feeds and databases. This is helpful for spotting potential security breaches and figuring out how big of an event it is.
- d Geolocation Information: In terms of IP addresses and domains, SpiderFoot may retrieve geolocation information. The physical location of servers or other equipment connected to the investigation can be tracked with the use of this information.
- e Vulnerability Scanning: It can find vulnerabilities that are known to be present in the target entities. Understanding potential attack vectors and security flaws is especially helpful in digital forensics.
- f Historical Information: SpiderFoot offers historical information that enables investigators to monitor changes to entities over time. This can be useful in figuring out how a target's online presence has changed over time.
- g Data Correlation: The tool can combine data from several sources to identify relationships and trends that might not be seen when looking at the data separately. This helps to provide a more thorough picture of the situation.
- h Dark Web Scanning: Searches for mentions of the target on the dark web.
- i Collaboration: Supports teamwork among investigators on the same case.

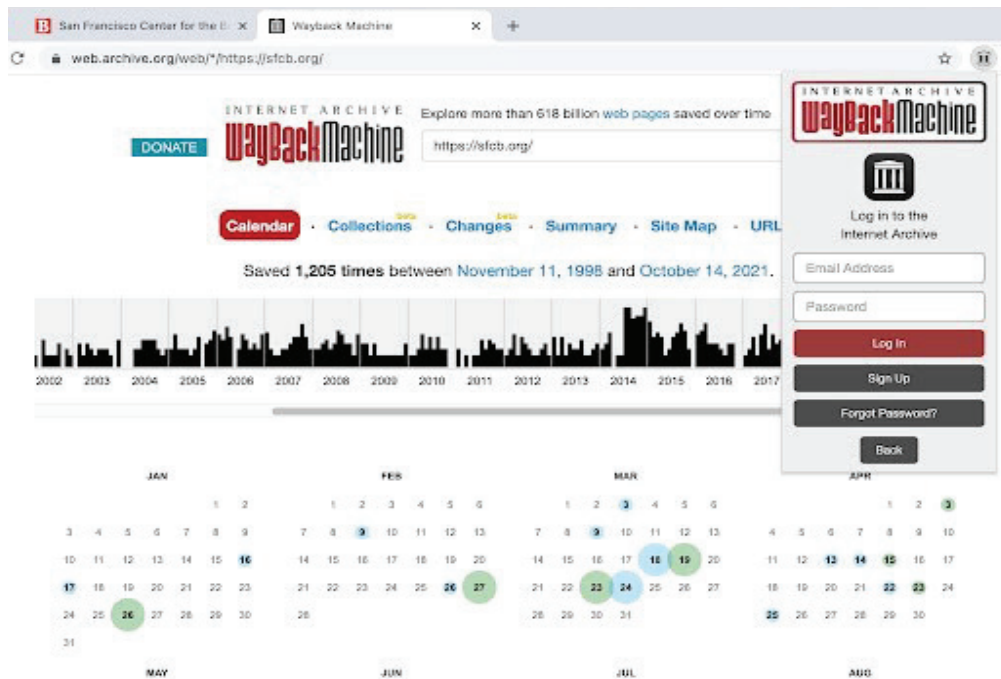
The screenshot shows the SpiderFoot web interface for a scan of 'Uber'. The interface includes a navigation bar with 'Summary', 'Correlations', 'Entities', 'Graph', 'Scan Settings', and 'Log'. Below the navigation bar is a table with the following columns: Type, Unique Data Elements, Total Data Elements, and Last Data Element. The table lists various data types and their corresponding counts and last update times.

Type	Unique Data Elements	Total Data Elements	Last Data Element
Account or External Site	1000	1000	2023-04-08 15:27:02
Affiliate - Company Name	86	812	2023-04-08 15:27:15
Affiliate - Domain Name	1000	1175	2023-04-08 15:27:30
Affiliate - Domain IP(s)	752	753	2023-04-08 14:34:23
Affiliate - Email Address	173	331	2023-04-08 15:29:30
Affiliate - IP Address	905	909	2023-04-08 15:27:05
Affiliate - IP(s) Address	20	21	2023-04-08 15:29:05
Affiliate - Internet Name	1074	1149	2023-04-08 15:23:47
Affiliate - Internet Name - Unresolved	0	0	2023-04-08 09:31:42
Affiliate - Web Content	7	8	2023-04-08 10:34:49
Affiliate Description - Abstract	0	0	2023-04-08 14:22:35
Affiliate Description - Category	18	18	2023-04-08 14:22:35
App Store Entry	4	4	2023-04-08 09:35:24
BOIP AS Membership	18	97	2023-04-08 10:00:10
BOIP AS Ownership	2	3	2023-04-08 14:48:29
Bitcoin Address	1	1	2023-04-08 09:50:35
Bitcoin Balance	1	1	2023-04-08 09:51:28
Blockchain Affiliate Internet Name	10	10	2023-04-08 15:08:34

5 Wayback Machine

The Wayback Machine is a web archiving service provided by the Internet Archive. Its main function is to take and store screenshots of websites and web pages at different times. Here are some of the Wayback Machine's primary applications:

- a Website History: It allows users to view past versions of websites and web pages, providing a historical record of how a site has evolved over time.
- b Research: Researchers and scholars use the Wayback Machine to study changes in web content, track trends, and access historical data for academic purposes.
- c Content Recovery: Users can retrieve content that may have been deleted or altered on the internet, making it a valuable tool for content recovery.
- d Content Verification: It helps in verifying the authenticity and accuracy of web content by comparing current versions with archived snapshots.
- e Historical References: Journalists and writers use the Wayback Machine to provide historical references and context when reporting on events or trends.
- f Legal and Copyright Issues: It can be used as evidence in legal proceedings, intellectual property disputes, or cases involving online content.
- g Website Maintenance: Web developers and site owners use it to view previous versions of their websites and ensure they are functioning correctly.
- h Digital Forensics: In digital forensics investigations, it can be used to retrieve and verify historical web data as evidence.
- i Educational Purposes: Educators use it to teach students about the evolution of the internet and the importance of preserving web history.
- j Recreating Lost Websites: The Wayback Machine can assist in recreating websites that are no longer live on the internet.



7 Censys

Censys is a search engine that focuses on internet-connected devices and networks. It helps with network reconnaissance by identifying open ports, protocols, and SSL/TLS certificate information. In digital forensics, Censys can be applied as follows:

- a Asset Discovery: Censys may be used to find out everything connected to a target IP address or domain, including all devices and services. This aids in creating an inventory of resources pertinent to the research.
- b Vulnerability Assessment: It can find well-known flaws in services and products connected to networks. Digital forensics specialists can better comprehend potential attack vectors and security flaws with the use of this knowledge.
- c Historical Information: Censys offers historical information on devices and services. Through tracking changes in network configurations, investigators may be able to determine when an incident took place or when particular assets were compromised.
- d Indicators of Compromise (IoC) Identification: Investigators can search Censys for IoCs, such as malicious IP addresses or domains. This aids in locating an attack's origin or locating other compromised assets.
- e SSL/TLS Certificate Analysis: Censys is able to examine SSL/TLS certificates connected to a target. This is helpful for locating safe services, comprehending encryption procedures, and recognizing potential security flaws.
- f Network Mapping: It facilitates the mapping of a target organization's or entity's network infrastructure. This covers finding open ports, services, and subdomains on various devices.

The screenshot shows the Censys Software page with a table of vulnerabilities. The table has columns for Name, Version, Host Count, CVE Count, Highest Severity Score, and Tags. Several items are marked as 'NEW'.

Name	Version	Host Count	CVE Count	Highest Severity Score	Tags
awscli	2.0	2 Hosts	0	1	NEW
flux	-	2 Hosts	0	-	NEW
nginx	1.15.0 ▲ End of life	2 Hosts	1	4.3	NEW
OpenBSD OpenSSH	7.8p1	2 Hosts	11	8.3	NEW
Ubuntu Linux	18.04	2 Hosts	0	-	NEW
Apache Lucene	5.5.0	1 Host	0	-	NEW

8 ThreatCrowd

ThreatCrowd aggregates information from various sources to provide insights into domains, IP addresses, and more. It helps in understanding the security posture of a target entity.

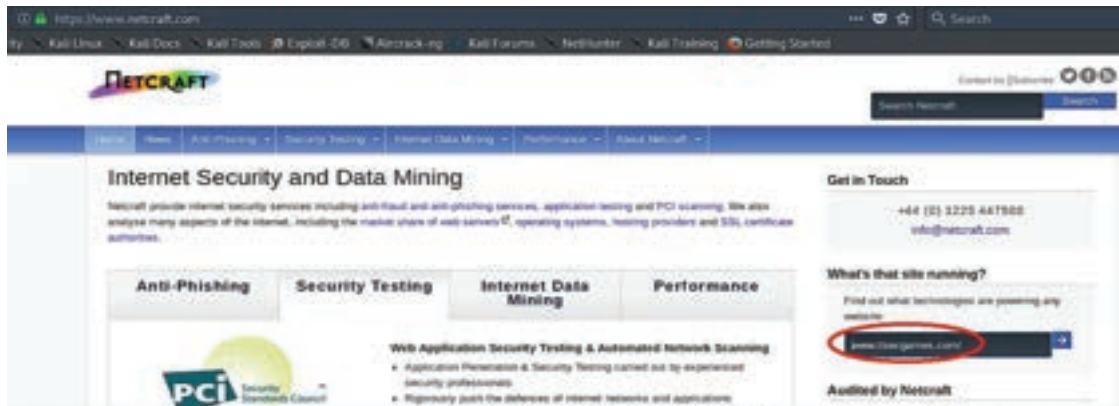
- a Data Aggregation: Collects threat data from multiple sources.
- b IoC Search: Helps find indicators of compromise (IoCs) like IP addresses and domains.
- c Malware Analysis: Provides insights into malware behavior and patterns.
- d Domain and IP Analysis: Analyzes reputation and history of websites and IPs.
- e Historical Data: Offers historical insights into threat evolution.
- f Phishing and Malicious URLs: Identifies and tracks phishing and malicious sites.
- g Threat Intelligence Sharing: Enables collaboration with the security community.
- h Alerts and Monitoring: Provides real-time threat alerts.
- i Digital Footprint Analysis: Tracks online presence of individuals and organizations.
- j Incident Response: Aids in incident scope identification and infrastructure tracking.
- k Threat Assessment: Assists in evaluating threat severity and impact.
- l Security Awareness: Educates security teams about emerging threats.



9 Netcraft

It is an internet service association that provides detailed data about the web facilitating and the Server with point-by-point data on what is running on the server alongside the IP, Whois data, server-side technologies, and so on. This information ought to be saved in your reports with the goal that you can utilize all the data to find the correct testing methodology and characterize the attack surface, which is the essential piece of a pentest.

- a Phishing Site Detection: Netcraft keeps an extensive database of recognized phishing sites. Professionals in digital forensics can utilize Netcraft's services to recognize and validate phishing sites, which is useful when looking into online fraud and criminality.
- b Malicious Website Analysis: Using the tools provided by Netcraft, you may examine websites for any indications of malicious behavior, including the presence of malware, shady redirects, and other security risks.
- c Site Reputation Analysis: Netcraft offers data on the reputation of websites and hosting infrastructure. This data may be useful for determining whether a website is trustworthy and for locating possibly compromised or malicious web servers.
- d SSL Certificate Analysis: Netcraft can be used by investigators to examine SSL/TLS certificates connected with websites. Understanding encryption procedures, recognizing secure services, and confirming the legitimacy of websites are all made easier thanks to this.
- e Historical Information: Netcraft keeps records on the infrastructure of websites throughout time. This might be helpful for monitoring changes, comprehending how web material changes over time, and looking into past instances.
- f DDoS Attack Monitoring: Netcraft provides tools and services to track Distributed Denial of Service (DDoS) attacks and identify targeted websites. Investigating cyberattacks and coordinating mitigation measures can both benefit from this.
- g Hosting Provider Identification: Netcraft is able to locate the data centers and hosting companies that are connected to specific IP addresses and websites. The source of cyberattacks or other malicious activity may be traced with the help of this information.
- h Email tracking: Netcraft offers services to monitor domains and email senders. This can be useful in figuring out where phishing emails or other email-based cyber risks are coming from.



10 Recon-ng

Recon-ng is a full-featured web reconnaissance framework. It includes numerous modules for gathering OSINT data from various sources and performing automated data analysis. Recon-ng is an open-source web reconnaissance framework that is primarily used by cybersecurity professionals and penetration testers for information gathering and reconnaissance, especially in the early stages of data collection and threat assessment. Here's how Recon-ng can be used in digital forensics:

- a **Passive Reconnaissance:** Recon-ng can perform passive reconnaissance by collecting publicly available information about a target, including domain names, subdomains, email addresses, and employee names. This information can be valuable in understanding the digital footprint of a target entity during the initial stages of an investigation.
- b **Open-Source Intelligence (OSINT) Gathering:** The framework integrates with various OSINT sources and modules, allowing investigators to gather data from social media, search engines, and other publicly accessible repositories. This information can help in profiling individuals or organizations under investigation.
- c **Metadata Collection:** Recon-ng can retrieve metadata from web pages and documents, which can be useful in verifying document authenticity, tracking document origins, and understanding document histories.
- d **Vulnerability Scanning:** While Recon-ng is not primarily a vulnerability scanner, it can be used to identify potential security weaknesses in a target's online presence. This information can be used to assess the attack surface and identify areas of potential vulnerability.
- e **Link Analysis:** The framework can be used to perform link analysis, helping investigators identify relationships and connections between different pieces of information. This can aid in uncovering patterns and associations in a digital forensics case.

```

recon-ng[mediac] > show dashboard
-----
| Activity Summary |
|-----|
| Module | Runs |
|-----|
| recon/domains-hosts/finding_domains_web | 1 |
| recon/domains-hosts/finding_subdomains | 1 |
| recon/domains-hosts/google_site_web | 1 |
| recon/hoste-hosts/ispinfo | 1 |
| recon/hoste-hosts/resolve | 2 |
| recon/locations-locations/geocode | 1 |
|-----|

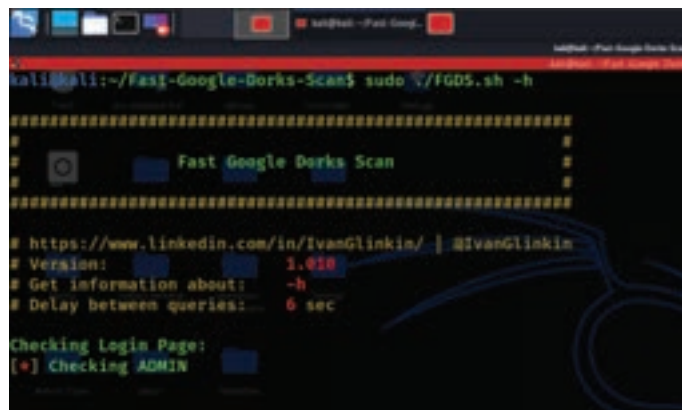
-----
| Results Summary |
|-----|
| Category | Quantity |
|-----|
| Domains | 1 |
| Companies | 0 |
| Websites | 0 |
| Locations | 0 |
| Vulnerabilities | 0 |
| Ports | 0 |
| Hosts | 04 |
| Contacts | 0 |
| Credentials | 0 |
| Links | 0 |
| Plugins | 0 |
| Profiles | 0 |
| Repositories | 0 |
|-----|
recon-ng[mediac] >

```

11 Google Dorks

Google Dorks can be a valuable tool in digital forensics for investigators and analysts to discover information and evidence related to a case. Google Dorks are specially crafted search queries that utilize Google's search engine to find specific information on the internet. Here's how Google Dorks can be used in digital forensic investigations:

- a Locating Sensitive Information: Google Dorks can help investigators locate sensitive information that should not be publicly accessible but may have been inadvertently exposed. This includes confidential documents, databases, login credentials, and more.
- b Identifying Vulnerabilities: Google Dorks can be used to search for websites and systems that have vulnerabilities or misconfigurations. This information can be crucial for understanding how a breach occurred or for proactively identifying security weaknesses.
- c Gathering Evidence: Investigators can use Google Dorks to search for specific keywords or file types related to a case. For example, they can search for documents, emails, or conversations that may contain evidence of a crime.
- d Tracking Online Activity: Google Dorks can help trace a suspect's online activity. By searching for specific usernames, email addresses, or other identifiers, investigators can link individuals to online accounts and activities.
- e Detecting Malware and Malicious Websites: Google Dorks can be used to identify websites hosting malware or to find indicators of compromise (IoCs) related to a cyberattack. This information can be used to analyze and mitigate security incidents.
- f Identifying Fake or Counterfeit Goods: In cases involving counterfeit products or intellectual property theft, Google Dorks can be used to locate websites selling counterfeit goods or distributing copyrighted material without permission.
- g Reconstructing Historical Data: Google Dorks can help reconstruct historical data by searching for cached or archived web pages. This can be useful when investigating cases involving deleted or modified online content.
- h Mapping Online Footprints: Investigators can use Google Dorks to map a person's or organization's online presence. This can include finding social media profiles, blog posts, forum comments, and other online activities



```
kali@kali:~/Fast-Google-Dorks-Scan$ sudo ./FGDS.sh -h
#####
#
#   Fast Google Dorks Scan
#
#####
# https://www.linkedin.com/in/IvanGlinkin/ | @IvanGlinkin
# Version: 1.010
# Get information about: -h
# Delay between queries: 6 sec

Checking Login Page:
[*] Checking ADMIN
```


12 Metagoofil

Metagoofil is a tool commonly used in digital forensics and cybersecurity to extract metadata from various file types, especially documents and media files. Metadata is information embedded within files that can provide valuable insights and evidence during an investigation. Here's how Metagoofil can be used for digital forensic purposes:

- a Collecting File Metadata: Metagoofil can be used to extract metadata such as author names, timestamps, document titles, and revision histories from a wide range of file formats, including Word documents, PDFs, images, and more.
- b Gathering Evidence: Digital forensics investigators can use Metagoofil to retrieve information that may be crucial in building a case. For example, the author's name or organization in a document's metadata may link it to a specific individual or entity.
- c Tracking Document Ownership: By analyzing document metadata, investigators can trace the ownership and history of files. This can be especially useful when determining the source of leaked or confidential information.
- d Determining File Origins: Metagoofil can help determine the source or origin of files found on a suspect's device or within a network. This information can be important for establishing the chain of custody and identifying potential sources of data breaches.
- e Assessing File Authenticity: Metadata can be used to verify the authenticity of a document or file. Investigators can check timestamps, document creation dates, and revision histories to determine if a file has been tampered with or is a forgery.
- f Locating Hidden Information: Some files may contain hidden or deleted information in their metadata that could be relevant to an investigation. Metagoofil can uncover this hidden data, which might otherwise go unnoticed.
- g Mapping Relationships: Metadata can reveal relationships between individuals, organizations, or files. Investigators can use this information to establish connections between different pieces of evidence.
- h Identifying Insider Threats: In cases involving insider threats or corporate espionage, Metagoofil can help identify employees or individuals responsible for leaking sensitive information by analyzing the metadata associated with the leaked documents.
- i Reconstructing File Histories: When investigating incidents involving data theft or data leakage, Metagoofil can help reconstruct the history of a file, including when it was created, modified, or accessed.



```
root@kali-2019:~# metagoofil
Metagoofil
Metagoofil Ver 2.2
Christian Martorella
Edge-Security.com
cmartorella@edge-security.com
usage: metagoofil options
-d: domain to search
-f: filetype to download (pdf, doc, xls, ppt, adp, ods, docx, xlsx, pptx)
```

Real-World Examples of OSINT Success

The potency of OSINT tools materializes through real-world case studies, elucidating their pivotal role in data aggregation, timeline establishment, and the revelation of concealed connections. These examples spotlight the pivotal contribution of OSINT tools in substantiating investigations and underpinning their efficacy.

7.8 HANDS ON TRAINING SCENARIOS WITH OSINT TOOLS

7.8.1 DESIGNING REALISTIC TRAINING SCENARIOS

Integral to OSINT training are hands-on scenarios that simulate real-world investigative challenges. Trainees confront hypothetical cases necessitating the acquisition of information from diverse online sources through OSINT tools. These scenarios mirror the complexities and uncertainties characteristic of actual cases, enhancing trainees' preparedness.

7.8.2 DEVELOPING PRACTICAL SKILLS THROUGH EXERCISES

Practical exercises constitute a cornerstone of OSINT training. Trainees are actively engaged in navigating online platforms, extracting pertinent information, and analyzing findings using OSINT tools. This immersive experience cultivates confidence, proficiency, and adeptness in problem-solving—essential attributes for conducting effective cyber forensics investigations.

7.8.3 ANALYZING AND INTERPRETING OSINT FINDINGS

A critical facet of OSINT proficiency lies in the adept analysis and interpretation of findings. Trainees acquire the acumen to contextualize information, recognize patterns, and derive substantial conclusions. This competency ensures that the insights harvested from OSINT channels significantly contribute to the investigative narrative.

7.9 ENHANCING INVESTIGATIONS WITH OSINT TOOLS

7.9.1 DIGITAL FOOTPRINT ANALYSIS

A central element of OSINT tools lies in the crafting of comprehensive digital footprints. Investigators wield OSINT tools to amalgamate information from diverse online sources, constructing an intricate mosaic that sheds light on an individual's or entity's online activities. This analytical process illuminates behavioral patterns, associations, and potential motivations.

7.9.2 SOCIAL MEDIA PROFILING

OSINT tools unfurl a tapestry of insights within the realm of social media platforms. Investigators plumb social media profiles, posts, and interactions, obtaining invaluable glimpses into an individual's interests, relationships, and the potential nexus between their online presence and cybercrimes.

7.9.3 EMAIL HEADER EXAMINATION

The quintessential communication medium, emails are pivotal in personal and professional interactions. OSINT tools facilitate the dissection of email headers, enabling investigators to trace the provenance, trajectory, and authenticity of an email. This scrutiny is pivotal in establishing the legitimacy and contextual relevance of email communications.

7.10 ETHICAL AND LEGAL CONSIDERATIONS IN OSINT

7.10.1 RESPECTING PRIVACY IN OSINT ACTIVITIES

The ethical underpinning of OSINT activities is paramount. Investigators tread the fine line between information acquisition and the preservation of individuals' privacy. Responsible OSINT practices abstain from intrusive or unethical data collection, embodying respect for privacy rights.

7.10.2 ADHERING TO LEGAL FRAMEWORKS

The ethical practice of OSINT extends to adherence to legal frameworks and regulations. Legal norms surrounding data protection, online privacy, and data collection are heterogeneous across jurisdictions. Investigators meticulously align their OSINT undertakings with these legal moorings to avert legal complications and safeguard the admissibility of evidence.

7.11 PREPARING FOR THE FUTURE: OSINT IN AN EVOLVING CYBER LANDSCAPE

7.11.1 ADAPTING TO TECHNOLOGICAL ADVANCEMENTS

In the midst of an ever-evolving digital panorama, OSINT tools must be agile to technological advancements. Novel technologies, platforms, and attack vectors necessitate the malleability of OSINT tools to ensure continued efficacy. Investigative professionals must remain poised to leverage emerging tools and techniques, perpetually augmenting their investigative prowess.

7.11.2 LIFELONG LEARNING AND SKILL DEVELOPMENT

The realm of cyber forensics is an indelibly dynamic landscape, demanding perpetual learning. Engaging in lifelong learning is requisite, involving active participation in workshops, immersion in online communities, and the exploration of novel tools and methodologies. This commitment to continuous growth is instrumental in maintaining the pertinence and effectiveness of OSINT in cyber forensics.

7.11.3 CONCLUSION

The assimilation of OSINT tools within the fabric of cyber forensics training programs bestows a transformative influence upon investigators' capacities. These tools empower investigators to adroitly gather external information, meticulously analyze its ramifications within the context of a case and glean profound insights. In a world witnessing the ascendancy of intricate cybercrimes, OSINT tools stand as an invaluable arsenal, equipping investigators with the wherewithal to unearth digital evidence, establish timelines, and unravel multifaceted cases. Through immersive training scenarios, ethical considerations, and the perpetual pursuit of knowledge, OSINT ascends to the status of an indispensable ally for contemporary cyber investigators, ensuring the perpetuation of a secure digital realm.



SUMMARY

In the digital age, the importance of digital forensics cannot be overstated. This field stands as a critical pillar in the realm of investigations, encompassing the systematic collection, preservation, analysis, and presentation of digital evidence. Its significance extends to resolving cybercrimes, supporting legal proceedings, and upholding the integrity of data. Modern investigations heavily rely on digital forensics tools, which streamline the intricate process of extracting, analysing, and interpreting digital evidence from diverse sources like computers, smartphones, and networks. These tools are indispensable, especially in the face of increasingly sophisticated cybercriminal activities, empowering investigators to uncover hidden insights and reconstruct digital events with precision.

Digital forensics tools span various categories, from those focused on disk and file analysis to memory and network analysis tools, malware analysis tools, and timeline generation tools. Their role is pivotal in ensuring the accurate collection, preservation, and analysis of digital evidence, making it admissible in legal proceedings while maintaining its integrity and authenticity. In today's landscape, the growing threat of cybercrime poses substantial challenges, demanding robust digital forensics practices. Cyber forensics experts must stay ahead to counteract the escalating complexity of cyberattacks. With a range of specialized digital forensics tools at their disposal, investigators can effectively address these challenges, safeguarding the security and reliability of digital evidence in an ever-evolving digital world.



REFERENCES

- 1 Lee Garber, "EnCase: A Case Study in Computer-Forensic Technology", *Computer Magazine*, Jan 2001.
- 2 EnCase tool, <https://www.guidancesoftware.com/encase-forensic>. Digital Forensics Framework tool, <http://www.arxsys.fr/features/>.
- 3 Pro-Discover tool, <http://www.arcgroupny.com/services/computerforensics/>. 2016].
- 4 X-Ways Forensics tool, <http://www.x-ways.net/forensics/>.
- 5 Quest change auditor tool, <https://www.quest.com/change-auditor/>
- 6 The Sleuth Kit, <http://www.sleuthkit.org/autopsy/features.php>. Forensic Toolkit, <http://accessdata.com/solutions/digitalforensics/forensic-toolkit-ftk>
- 7 Computer Online Forensic Evidence Extractor, <https://cofee.nw3c.org/>. [Accessed: 28-Oct- 2016].
- 8 Bulk Extractor, <http://tools.kali.org/forensics/bulk-extractor>. [Accessed: 10- Nov- 2016].
- 9 July 2021, Joel Khalili 31. "Cellebrite: The mysterious phone-cracking company that insists it has nothing to hide". *TechRadar*. Archived from the original on 2021-07-31. Retrieved 2021-09-07.
Information Technology -- New Generations: 15th International Conference on Information Technology. Shahram Latifi. Cham, Switzerland. 2018. p. 82. ISBN978-3-319-77028-4 OCLC 1031400154.
- 10 <https://cellebrite.com/en/cellebrite-physical-analyzer-ultra/#:~:text=Physical%20Analyzer%20Ultra's%20tabbed%20interface,artifact%20type%20separate%20and%20organized.&text=Descriptive%20labels%20to%20help%20identify%20important%20location%20data.&text=Descriptive%20labels%20to%20help%20identify%20important%20location%20data,-Multi%20DTabbed%20Interface>
- 11 <https://www.dataexpert.eu/products/cloud-forensics-cellebrite/cellebrite-physical-analyzer/>
- 12 <https://www.oreilly.com/library/view/practical-mobile-forensics/9781788839198/1d7e4d41-23be-49f5-b545-df75978d15a8.xhtml>
- 13 <https://teeltech.com/mobile-device-forensic-tools/cellebrite/ufed-physical-analyzer/>
- 14 Techniques and tools for OSINT-based threat analysis

CHAPTER 8

DIGITAL FORENSICS IN AUDITING & FORENSIC ACCOUNTING



LEARNING OBJECTIVES

- Develop a profound understanding of integrating digital forensics techniques into financial investigations.
- Acquire skills to apply digital forensic methodologies for identifying financial irregularities.
- Learn to utilize specialized tools for in-depth data analysis in the context of financial investigations.
- Gain the ability to navigate complex ethical considerations and data privacy concerns related to digital evidence.
- Understand the application of digital forensic skills in real-world case studies to uncover financial irregularities.
- Stay updated with emerging trends in the field of digital forensics and their impact on financial investigations.
- Integrate acquired skills seamlessly into professional roles within auditing and forensic accounting contexts.

8.1 INTRODUCTION: CONVERGENCE OF DIGITAL FORENSICS, AUDITING, AND FORENSIC ACCOUNTING

Digital forensics, auditing, and forensic accounting are three closely related disciplines that are increasingly converging to help organizations detect and investigate financial irregularities.

- Digital forensics is the process of collecting, preserving, analysing, and presenting digital evidence. It is used to investigate a wide range of crimes, including fraud, hacking, and intellectual property theft.
- Auditing is a systematic process of examining financial records to ensure that they are accurate and reliable. It is used to ensure that organizations are complying with laws and regulations, and to detect fraud and other financial irregularities.
- Forensic accounting is the application of accounting principles to legal matters. It is used to reconstruct financial transactions, identify fraud, and assess damages.

The convergence of these three disciplines is being driven by the increasing digitization of financial records. As more and more financial transactions are conducted electronically, digital forensics techniques are becoming increasingly important for investigators.

For example, digital forensics can be used to recover deleted files, track email communications, and analyze financial transactions. This information can be used by auditors and forensic accountants to identify fraud and other financial irregularities.

The convergence of digital forensics, auditing, and forensic accounting is a positive development for organizations. It provides them with a more comprehensive and effective way to detect and investigate financial irregularities.

8.2 DIGITAL EVIDENCE'S ROLE IN DETECTING FINANCIAL ANOMALIES AND FRAUD

Digital evidence is any electronic data that can be used to prove or disprove a fact in a legal proceeding. It can include emails, text messages, financial records, and other electronic documents.

Digital evidence is becoming increasingly important in financial investigations. This is because more and more financial transactions are being conducted electronically. As a result, there is a growing amount of digital evidence that can be used to track financial activity and identify fraud.

For example, digital evidence can be used to:

- Trace the movement of money
- Identify patterns of suspicious activity
- Recover deleted files
- Establish a timeline of events
- Identify the perpetrators of fraud

Digital evidence can be a powerful tool for investigators. However, it is important to collect and preserve digital evidence properly in order to ensure that it is admissible in court.



8.3 SPECIALIZED SKILLS IN MODERN FINANCIAL INVESTIGATIONS

The landscape of financial crimes has changed significantly in recent years. As a result, investigators need to have specialized skills in order to effectively investigate these crimes.

Some of the specialized skills that are essential for modern financial investigators include:

- **Financial expertise:** Investigators need to have a strong understanding of financial concepts and terminology. This will help them to identify suspicious financial activity and to understand the implications of the evidence that they collect.
- **Technological skills:** Investigators need to be proficient in using digital forensics tools and techniques. This will allow them to collect and analyze digital evidence effectively.
- **Legal knowledge:** Investigators need to have a strong understanding of the laws and regulations that apply to financial investigations. This will help them to ensure that their investigations are conducted in a lawful manner.
- **Behavioural insights:** Investigators need to be able to understand the psychology of fraudsters. This will help them to identify the motives and methods of fraudsters and to develop strategies for preventing and detecting fraud.
- **Cultural awareness:** Investigators need to be aware of the cultural factors that can influence financial crimes. This will help them to understand the context of the crimes that they are investigating and to develop strategies that are appropriate for the specific cultural environment.

In addition to these specialized skills, modern financial investigators also need to be able to think critically and creatively. They need to be able to identify patterns and trends in data, and to develop innovative strategies for investigating financial crimes.

They also need to be able to work effectively with other professionals, such as lawyers, accountants, and law enforcement officers.

The field of financial investigations is constantly evolving, and investigators need to be prepared to adapt to new challenges. By developing the specialized skills and knowledge that are essential for this field, investigators can play a vital role in protecting organizations from financial crime.

Analyzing Financial Data using Digital Forensics

Ratio analysis: Ratio analysis is a method of comparing financial data points to each other to assess a company's financial health. For example, a company's debt-to-equity ratio can be compared to industry benchmarks to see how much debt the company is carrying relative to its equity.

Ratio analysis: Ratio analysis is a method of comparing financial data points to each other to assess a company's financial health. For example, a company's debt-to-equity ratio can be compared to industry benchmarks to see how much debt the company is carrying relative to its equity.

Time series analysis: Time series analysis is a method of analysing trends in financial data over time. This can be used to identify patterns and make predictions about future performance. For example, a company's sales data could be analysed to see if there are any seasonal trends or if the sales are growing or declining.

Correlation and regression analysis: Correlation and regression analysis are methods of identifying relationships between different financial variables. For example, a company's sales data could be correlated with its marketing spending data to see if there is a relationship between the two variables.

Cluster analysis: Cluster analysis is a method of grouping similar data points together. This can be used to identify patterns in financial data. For example, a company's customer data could be clustered to identify different customer segments.

Benford's law: Benford's law is a statistical law that states that the first digit of many naturally occurring numbers follows a specific distribution. This can be used to detect fraud or errors in financial data. For example, if the first digit of a large number of financial transactions is 1 more often than would be expected by chance, this could be a sign of fraud.

Module 2: Practical Demonstration of Digital Tools

Data mining software: Data mining software can be used to extract patterns and trends from large datasets. This can be used to identify fraud, identify customer behaviour, and make predictions about future performance.

Data visualization software: Data visualization software can be used to create charts and graphs to help visualize the results of financial data analysis. This can make the results of the analysis easier to understand and communicate.

Fraud detection software: Fraud detection software can be used to identify fraudulent transactions in financial data. This can help to protect businesses from financial losses.

Module 3: Advantages and Limitations of Financial Data Analysis

Advantages:

- **Improved decision-making:** By identifying trends and patterns in financial data, businesses can make more informed decisions about their financial planning and strategies.
- **Increased efficiency:** Financial data analysis can help businesses to identify areas where they can improve efficiency and save money.
- **Reduced risk:** By identifying potential risks, businesses can take steps to mitigate those risks.
- **Enhanced fraud detection:** Financial data analysis can be used to identify fraudulent transactions, which can help to protect businesses from financial losses.

Limitations:

- **Data quality:** The quality of the data used for financial data analysis is essential for the accuracy of the results. If the data is inaccurate or incomplete, the results of the analysis will be unreliable.
- **Assumptions and biases:** The results of financial data analysis can be influenced by the assumptions and biases of the analyst. It is important to be aware of these assumptions and biases and to take steps to mitigate their impact.
- **Limited context:** The results of financial data analysis should be interpreted in the context of the specific business or industry. The results of an analysis of a company in the technology sector may not be applicable to a company in the manufacturing sector.
- **Overfitting:** Financial data analysis models can be overfit to the data, which can lead to inaccurate results. Overfitting occurs when the model is too closely tuned to the specific data that it was trained on. This can make the model unable to generalize to new data.
- **Changing environment:** The results of financial data analysis can be affected by changes in the business environment. For example, a change in interest rates can have a significant impact on a company's financial performance.

Conclusion

Financial data analysis is a powerful tool that can be used to gain insights into financial data. However, it is important to be aware of the limitations of this technique and to use it in conjunction with other methods of financial analysis.

Additional considerations for chartered accountants Chartered accountants (CAs) play an important role in financial data analysis. They use their knowledge of financial accounting and auditing to interpret the results of financial data analysis and to make recommendations to businesses.

CAs should also be aware of the ethical considerations of financial data analysis. They should ensure that they use this technique in a way that is fair and objective, and that they protect the privacy of the individuals and businesses involved.



Here are some additional considerations for chartered accountants:

- The need for technical expertise: CAs need to have a strong understanding of the statistical and mathematical methods used in financial data analysis. This includes knowledge of regression analysis, time series analysis, and clustering algorithms.
- The need for domain knowledge: CAs need to have a strong understanding of the specific business or industry that they are analysing. This includes knowledge of the industry's terminology, regulations, and best practices.
- The need for ethical judgment: CAs need to use financial data analysis in a way that is ethical and responsible. This includes protecting the privacy of the individuals and businesses involved, and avoiding conflicts of interest.

The importance of data quality: The quality of the data used for financial data analysis is essential for the accuracy of the results. CAs should carefully review the data to ensure that it is accurate and complete.

Here are some tips for ensuring data quality:

- Identify the data sources: The first step is to identify the data sources that will be used for the analysis. This includes both internal and external data sources.
- Clean the data: Once the data sources have been identified, the data needs to be cleaned. This includes removing errors, duplicates, and outliers.
- Validate the data: The data should then be validated to ensure that it is accurate and consistent. This can be done by comparing the data to other sources or by using statistical tests.
- Document the data: The data should be documented so that it can be easily traced back to the original source. This will help to ensure the accuracy of the analysis.
- The need for continuous learning: The field of financial data analysis is constantly evolving, so CAs need to be willing to learn new techniques and methods. This can be done by attending conferences, reading industry publications, and taking online courses.
- The importance of collaboration: Financial data analysis is often a team effort, so CAs need to be able to collaborate effectively with other professionals, such as data scientists and auditors. This requires the ability to communicate effectively, share ideas, and work together towards a common goal.
- By understanding these considerations, CAs can use financial data analysis to make informed decisions and provide valuable insights to their client.
- Financial data analysis is a powerful tool that can be used to gain insights into financial data. It can be used to identify trends, patterns, and anomalies in financial data. This information can be used to make informed decisions about financial planning and strategies, identify potential risks, and prevent fraud.
- Chartered accountants (CAs) play an important role in financial data analysis. They use their knowledge of financial accounting and auditing to interpret the results of financial data analysis and to make recommendations to businesses.

CAs should also be aware of the ethical considerations of financial data analysis. They should ensure that they use this technique in a way that is fair and objective, and that they protect the privacy of the individuals and businesses involved.

To be successful in financial data analysis, CAs need to have a strong understanding of the statistical and mathematical methods used in financial data analysis, as well as the specific business or industry that they are analyzing. They also need to be aware of the ethical considerations of financial data analysis and be willing to learn new techniques and methods.

By understanding these considerations, CAs can use financial data analysis to make informed decisions and provide valuable insights to their clients.

8.4 BALANCING INVESTIGATIVE NEEDS WITH ETHICAL CONSIDERATIONS

- Navigating Ethical Quandaries
 - Privacy vs. Investigation: Investigations often intrude on personal lives, sparking ethical concerns. Balancing privacy and information needs involves careful deliberation on respecting individual rights while obtaining necessary evidence.
 - Informed Consent in Digital Forensics: Extracting digital evidence raises questions of consent. Ethical concerns center on how individuals are informed about data extraction. Ensuring informed, voluntary consent becomes crucial.
- Transparency as a Guiding Principle
 - Communication with Stakeholders: Transparency builds trust by communicating with victims, suspects, and legal representatives. Openness about progress, scope, and potential outcomes enhances accountability and understanding.
 - Comprehensive Documentation: Transparent investigations require detailed records of actions, evidence, and decisions. Documentation ensures accountability and showcases ethical conduct.
- Accountability in the Pursuit of Justice
 - Unbiased Analysis: Maintaining unbiased analysis ensures investigative integrity. Objectivity throughout evidence collection, analysis, and presentation is essential for accountability.
 - Ethical Review Boards: Independent ethical review boards offer an extra layer of accountability in sensitive cases. They assess methods and guide ethical decisions.
- Strategies for Balance
 - Ethics Training for Investigators: Ongoing ethics training fosters awareness and critical thinking in ethical decision-making, preparing investigators to navigate complex challenges.
 - Ethics Consultation: Offering ethics guidance prevents missteps. Peers, mentors, or ethics experts help investigators make informed ethical choices.

8.5 ENSURING COMPLIANCE WITH DATA PROTECTION REGULATIONS

- Complex Data Protection Landscape
 - GDPR and Beyond: Global regulations like GDPR and CCPA mandate strict data handling rules. Organizations must navigate this complex landscape when operating internationally.
 - Individual Rights: Data protection empowers individuals with rights over their data, requiring organizations to respect and uphold these rights.
- Data Extraction and Compliance
 - Legal and Ethical Considerations: Data extraction must balance needs and ethics, adhering to regulations while protecting privacy.
 - Minimization and Anonymization: Collecting minimal data and anonymization safeguards privacy and minimizes risks.
- Preservation
 - Chain of Custody: Data preservation relies on a robust chain of custody. Accurate documentation ensures integrity and legal admissibility.
 - Secure Storage: Secure measures like encryption and access controls protect data and demonstrate commitment to data protection.
- Strategies for Compliance
 - Data Protection Officers (DPOs): DPOs oversee data protection, offer guidance, and ensure practices align with regulations.
 - Data Protection Impact Assessments (DPIAs): Assessing data processes identifies risks, mitigates non-compliance, and demonstrates responsible data handling.



8.6 SAFEGUARDING DATA INTEGRITY AND PRIVACY

- Data Integrity Assurance
 - Ensuring Accuracy: Data integrity maintains accuracy throughout its lifecycle. Error prevention and consistency are crucial.
 - Assurance Methods: Techniques like checksums, hashing, and encryption contribute to data integrity.
- Privacy by Design
 - Proactive Privacy: Integrating privacy from the start prevents retroactive adjustments that compromise privacy.
 - Default Privacy Settings: Privacy-centric default settings prevent excessive data collection.
- Ensuring Data Integrity and Privacy
 - Access Controls: Robust controls limit access, maintaining integrity and preventing breaches.
 - Data Encryption: Encryption safeguards data integrity and privacy during transmission and storage.
 - Regular Audits: Audits ensure compliance, identify vulnerabilities, and assess data practices.
- Benefits of Holistic Approach
 - A holistic approach to data privacy and ethics ensures that all aspects of data handling are considered, from collection to disposal.
 - This approach helps to protect individual rights, build trust, and mitigate risks.

By understanding the ethical considerations and data privacy principles outlined in this chapter, chartered accountants can play a vital role in ensuring that data is handled responsibly and ethically.

Here are some additional resources that chartered accountants may find helpful:

- The International Association of Privacy Professionals (IAPP): <https://iapp.org/>
- The European Union General Data Protection Regulation (GDPR): <https://gdpr-info.eu/>
- The California Consumer Privacy Act (CCPA): <https://oag.ca.gov/privacy/ccpa>
- The National Institute of Standards and Technology (NIST) Special Publication 800-53: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>
- The context in which data is being collected and used is important. For example, data collected for marketing purposes may have different ethical implications than data collected for medical research.
- The sensitivity of the data is also a factor. For example, data about an individual's health or finances is more sensitive than data about their favourite sports team.
- The purpose for which the data is being used is also important. For example, data that is being used for legitimate purposes, such as fraud prevention, may have different ethical implications than data that is being used for more nefarious purposes, such as discrimination.

- The impact of the data collection and use on individuals and society is also important to consider. For example, data collection that could lead to discrimination or other harm to individuals would be considered unethical.

It is important to remember that there is no one-size-fits-all answer to the question of ethical data collection and use. The specific ethical considerations will vary depending on the context, the sensitivity of the data, the purpose for which the data is being used, and the impact of the data collection and use on individuals and society.

As a chartered accountant, you have a responsibility to uphold the highest ethical standards in your work. This includes ensuring that data is collected and used ethically. By understanding the ethical considerations and data privacy principles outlined in this chapter, you can play a vital role in protecting individual rights and ensuring the responsible and ethical use of data.

Here are some specific things that chartered accountants can do to ensure ethical data collection and use:

- Be aware of the ethical considerations involved in data collection and use. This includes understanding the different types of data, the different ways that data can be used, and the potential ethical implications of each.
- Get consent from individuals before collecting their data. This consent should be informed and voluntary, and it should be clear how the data will be used.
- Use data only for the purposes for which it was collected. Do not use data for any other purposes without the consent of the individual.
- Protect data from unauthorized access, use, or disclosure. This includes using appropriate security measures to protect the data.
- Delete data when it is no longer needed. Do not keep data longer than necessary.
- Be transparent about data collection and use practices. This includes providing individuals with information about how their data is being collected and used.
- **Accountability:** Chartered accountants have a responsibility to be accountable for their actions in relation to data privacy and ethics. This means that they should be able to explain and justify their decisions, and they should be willing to take responsibility for any mistakes or breaches.
- **Proactiveness:** Chartered accountants should be proactive in their approach to data privacy and ethics. This means that they should not wait for problems to arise before taking action. They should be constantly reviewing their data handling practices and procedures to ensure that they are up-to-date and compliant with the latest regulations.

- Innovation: Chartered accountants should be willing to innovate in their approach to data privacy and ethics. This means that they should not be afraid to try new things and to explore new ways of working. They should be open to new technologies and new ways of thinking about data privacy and ethics.
- Collaboration: Chartered accountants should collaborate with others to address data privacy and ethics challenges. This means working with other professionals, such as lawyers, IT experts, and privacy officers, to develop solutions that are effective and sustainable.
- Education: Chartered accountants should educate themselves and others about data privacy and ethics. This means staying up-to-date on the latest regulations and trends, and sharing this knowledge with others. They should also be willing to help others to understand the importance of data privacy and ethics.



By following these principles, chartered accountants can help to ensure that they are upholding the highest ethical standards in their work and that they are playing a vital role in protecting individual rights and ensuring the responsible and ethical use of data.

In addition to the above, here are some specific things that chartered accountants can do to stay up-to-date on data privacy and ethics:

- Attend training and workshops on data privacy and ethics.
- Read industry publications and journals on data privacy and ethics.
- Join professional organizations that focus on data privacy and ethics.
- Network with other professionals who are working in the field of data privacy and ethics.
- The role of technology in data privacy is evolving rapidly. New technologies, such as artificial intelligence and blockchain, are being used to collect, store, and analyze data in ways that were not possible before. This raises new ethical challenges, such as how to ensure that these technologies are used in a fair and responsible way.
- The globalization of data is also a challenge for data privacy. Data is increasingly being collected and stored across borders, which makes it more difficult to regulate and protect. This is especially true in the case of cross-border data transfers, where the laws of different countries may conflict.
- The rise of data activism is another challenge for data privacy. Individuals and groups are increasingly using data to hold organizations accountable for their data handling practices. This can put pressure on organizations to improve their data privacy practices, but it can also lead to conflicts between the rights of individuals and the needs of organizations.

Chartered accountants need to be aware of these challenges and trends in order to stay ahead of the curve and protect the privacy of their clients and their own businesses. They also need to be prepared to adapt their practices as the landscape of data privacy continues to evolve.

Here are some specific things that chartered accountants can do to address the challenges of data privacy:

- Stay up-to-date on the latest regulations and trends. This includes understanding the different data privacy laws and regulations that apply to their work, as well as the latest technologies and trends that are affecting data privacy.
- Be transparent about their data handling practices. This means providing clients with clear information about how their data is being collected, used, and stored.
- Use appropriate security measures to protect data. This includes using encryption, access controls, and other measures to prevent unauthorized access to data.
- Be proactive in responding to data breaches. This means having a plan in place to respond to data breaches in a timely and effective manner.
- Work with clients to develop and implement data privacy policies and procedures. This can help to ensure that clients are taking steps to protect their own data privacy.



SUMMARY

The convergence of digital forensics, auditing, and forensic accounting is a response to the increasing digitization of financial records, enabling organizations to effectively detect and investigate financial irregularities. This alignment leverages digital forensics' capabilities in collecting and analysing digital evidence, which is vital for probing crimes like fraud and hacking. Auditing ensures financial records' accuracy and compliance with regulations, aiding in fraud detection, while forensic accounting applies accounting principles to legal matters, helping reconstruct financial transactions and assess damages. As financial transactions become increasingly electronic, these disciplines' integration provides a comprehensive approach, where digital evidence plays a pivotal role, specialized skills are essential, and ethical considerations are paramount in maintaining transparency and accountability in financial investigations. Compliance with data protection regulations is crucial, emphasizing minimization and anonymization of data, secure storage, and ethical data handling practices. Safeguarding data integrity and privacy involves error prevention, proactive privacy measures, access controls, data encryption, and regular audits. Chartered accountants, possessing a unique role, must navigate these complexities while upholding ethical standards, ensuring data is collected and used responsibly, and staying updated on evolving data privacy challenges.



REFERENCES

- 1 *Contemporary Issues in Audit Management and Forensic Accounting*
- 2 *Fraud Investigation and Forensic Accounting in the Real World*
- 3 *Data Sleuth: Using Data in Forensic Accounting Engagements and Fraud Investigations*

MCQ AND DESCRIPTIVE QUESTION & ANSWERS

Chapter 1

Multiple Choice Questions (MCQ) for Practice

- 1 Which of the following best defines cybercrime?
 - a) Theft using a computer.
 - b) Any attack on information systems.
 - c) Simply browsing the internet.
 - d) Physical damage to a computer.

- 2 Which type of cyber-attack involves unauthorized discovery and mapping of systems or vulnerabilities?
 - a) Reconnaissance
 - b) Access
 - c) Denial of service
 - d) Malware

- 3 Which is NOT a reason for the commission of cybercrimes?
 - a) Money
 - b) Recognition
 - c) Convenience
 - d) Revenge

- 4 What do cyber warfare and cyber terrorism have in common?
 - a) Both are non-destructive.
 - b) Both target individual users primarily.
 - c) Both are related to cyberspace conflicts between India and Pakistan.
 - d) Both aim to damage critical infrastructures within cyberspace.

- 5 Which term is used to describe a person who sends multiple unsolicited messages to various recipients?
 - a) Phisher
 - b) Hacker
 - c) Spammer
 - d) Trojan

- 6 What does the term 'phishing' typically refer to?
 - a) Spreading malware via email.
 - b) Sending unsolicited advertisements.
 - c) Trickery to gain sensitive information.
 - d) Programming for fishing simulations.

- 7 Which term describes an individual who manipulates the phone network for unauthorized purposes?
- a) Hacker
 - b) Spammer
 - c) Phreaker
 - d) Phisher
- 8 What is the main difference between viruses and worms?
- a) Worms are self-replicating.
 - b) Viruses are self-replicating.
 - c) Worms damage files.
 - d) Viruses cannot spread to other computers.
- 9 Which of the following attacks is designed to saturate network links with spurious data?
- a) Reconnaissance
 - b) Access
 - c) Denial of Service (DoS)
 - d) Malware
- 10 What term is used for a computer compromised in a botnet?
- a) Victim
 - b) Robot
 - c) Zombie
 - d) Ghost
- 11 Which cybercrime involves the act of registering a domain name intending to profit from someone else's trademark?
- a) Cyberbullying
 - b) Cyber-squatting
 - c) Phishing
 - d) Espionage
- 12 Which of the following attacks uses compromised hosts to pass traffic through a firewall?
- a) Trust Exploitation
 - b) Port Redirection
 - c) Man-in-the-Middle
 - d) Password Attack
- 13 A malicious software that appears to perform one function but acts as something else is known as?
- a) Virus
 - b) Worm
 - c) Trojan horse
 - d) Spyware

- 14 Cyber Security is the preservation of which of the following in the cyberspace?
- a) Confidentiality, Malware, and Destruction
 - b) Accessibility, Integrity, and Destruction
 - c) Confidentiality, Integrity, and Availability
 - d) Accessibility, Malware, and Prevention
- 15 Which term is used to describe a fraudulent phone call attempting to gain personal information?
- a) Phishing
 - b) Vishing
 - c) Smishing
 - d) Hacking

Answers

- 1 b) *Any attack on information systems.*
- 2 a) *Reconnaissance*
- 3 c) *Convenience*
- 4 d) *Both aim to damage critical infrastructures within cyberspace.*
- 5 c) *Spammer*
- 6 c) *Trickery to gain sensitive information.*
- 7 c) *Phreaker*
- 8 a) *Worms are self-replicating.*
- 9 c) *Denial of Service (DoS)*
- 10 c) *Zombie*
- 11 b) *Cyber-squatting*
- 12 b) *Port Redirection*
- 13 c) *Trojan horse*
- 14 c) *Confidentiality, Integrity, and Availability*
- 15 b) *Vishing*



SELF-EXAMINATION QUESTIONS FOR PRACTICE

- 1 How is cybercrime defined, and what types of attacks does it encompass?
- 2 Differentiate between a cyber-campaign, cyber warfare, and cyber terrorism. Which of these poses the most extensive threat to national infrastructures?
- 3 What are the primary differences between cyber warfare and cyber terrorism in terms of their objectives and outcomes?
- 4 Define Cyber Security. Why is it essential in preserving the confidentiality, integrity, and availability of information in cyberspace?
- 5 List and explain three primary motivations behind individuals or entities committing cybercrimes.

- 6 Distinguish between a 'white hat' and a 'black hat'. Which of them has malicious intentions, and which one aims to help?
- 7 Define and differentiate between Viruses, Worms, and Trojan horses.
- 8 What does the term "Denial of Service" imply in the context of cyber-attacks? How does a Distributed Denial-of-Service (DDoS) attack differ from a standard DoS attack?
- 9 Describe the fraudulent activity involved in 'Phishing' and explain how it's different from 'Vishing'.
- 10 Briefly explain the cyberspace conflicts that have historically occurred between India and Pakistan, starting from the 1990s.

Chapter 2**Multiple Choice Questions (MCQ) for Practice**

- 1 The growing dependence on the Internet has led to:
 - a) Reduced communication
 - b) A decline in traditional crimes
 - c) Increased cybercrimes
 - d) Reduced online shopping

- 2 Which sector has seen a significant rise in cyber incidents and data breaches in recent years?
 - a) Manufacturing
 - b) Healthcare
 - c) Digital Financial Services
 - d) Education

- 3 What can result in financial and psychological harm for customers?
 - a) High transaction rates
 - b) Positive user reviews
 - c) Falling victim to a scam
 - d) Discounts on services

- 4 What did the 2016 survey by ITU and CGAP reveal about the Philippine respondents?
 - a) 5% received fraudulent SMSs
 - b) 56% received fraudulent SMSs
 - c) 83% received fraudulent SMSs
 - d) 12% received fraudulent SMSs

- 5 Who have recognized the risk of cybercrime in the financial sector?
 - a) Local banks
 - b) G7 and G20 Finance Ministers
 - c) E-commerce companies
 - d) Educational institutions

- 6 Which of the following was a recent trending cybercrime attack?
 - a) Digital painting
 - b) Cloud storage breach
 - c) Ransomware Attacks
 - d) GPS hacking

- 7 What is the primary aim of a supply chain attack?
- a) Increase the supply chain
 - b) Cause harm by infiltrating a weak point in the system
 - c) Improve the supply chain network
 - d) Decrease the price of products
- 8 Whaling attacks specifically target:
- a) Small businesses
 - b) Senior executives
 - c) Junior employees
 - d) External vendors
- 9 Which pandemic led to an increase in cybercriminal opportunities related to remote work vulnerabilities?
- a) SARS
 - b) H1N1
 - c) Ebola
 - d) COVID-19
- 10 Insider threats can be:
- a) Always unintentional
 - b) Always external
 - c) Intentional or unintentional
 - d) Only during work hours
- 11 Multi-factor authentication (MFA) is a core element of:
- a) Threat detection
 - b) Supply chain management
 - c) Identity and access management
 - d) Crisis management
- 12 Which measure helps organizations maintain greater control over financial transactions?
- a) Single controls
 - b) Dual and triple controls
 - c) Zero-trust network model
 - d) Periodic auditing
- 13 To detect supply chain attacks, organizations should create a:
- a) Social media campaign
 - b) Product catalog
 - c) Threat model
 - d) New supply chain

- 14 Which financial institution was involved in a scam in 2018?
- a) Bank of America
 - b) Punjab National Bank
 - c) Barclays
 - d) Deutsche Bank
- 15 Zero-trust network model is crucial for:
- a) Expanding the network
 - b) Adding more employees
 - c) Limiting liabilities in the event of a network intrusion
 - d) Increasing the speed of transactions

Answers

- 1 c) *Increased cybercrimes*
- 2 c) *Digital Financial Services*
- 3 c) *Falling victim to a scam*
- 4 c) *83% received fraudulent SMSs*
- 5 b) *G7 and G20 Finance Ministers*
- 6 c) *Ransomware Attacks*
- 7 b) *Cause harm by infiltrating a weak point in the system*
- 8 b) *Senior executives*
- 9 d) *COVID-19*
- 10 c) *Intentional or unintentional*
- 11 c) *Identity and access management*
- 12 b) *Dual and triple controls*
- 13 c) *Threat model*
- 14 b) *Punjab National Bank*
- 15 c) *Limiting liabilities in the event of a network intrusion*



SELF-EXAMINATION QUESTIONS FOR PRACTICE

- 1 What is the primary reason for the increased dependency on the Internet in recent years, and how has this contributed to the rise of cybercrimes?
- 2 How has cybercrime affected the progress of financial inclusion in developing countries?
- 3 According to research, how does network or service downtime impact the behavior of low-income mobile money users?
- 4 Which international bodies, such as the G7 and G20, have recognized the risk of cybercrime in the financial sector?
- 5 What is the main distinction between regular phishing and spear phishing?
- 6 Why did the shift to remote work during the COVID-19 pandemic create new vulnerabilities for cyberattacks?

- 7 How does CISA define an "insider threat," and what are some potential harmful outcomes of such a threat?
- 8 How can multi-factor authentication (MFA) contribute to securing financial institutions' accounts from potential threats?
- 9 In the Punjab National Bank scam of 2018, which unauthorized financial instrument was fabricated by a junior PNB staff member to facilitate the fraud?
- 10 Why does the cross-border nature of many cyberattacks pose a significant challenge to the financial sector?

CHAPTER 3**Multiple Choice Questions (MCQ) for Practice**

- 1 What does Modus Operandi refer to in cybercrime?
 - a) Typical methods used by cyber professionals.
 - b) Typical methods used by cybercriminals.
 - c) General behaviour of internet users.
 - d) Common cybersecurity software.

- 2 Which of these is NOT one of the core elements every Modus Operandi contains?
 - a) Ensure success of the crime.
 - b) Protect and identity.
 - c) Purchase advanced software.
 - d) Effect Escape.

- 3 What was the primary method of attack in the Dani Data app scam?
 - a) DDoS Attack.
 - b) Malware.
 - c) Ransomware.
 - d) Ponzi scheme.

- 4 Which cyberattack technique was most frequent, accounting for 37%?
 - a) Spam emails.
 - b) Phishing.
 - c) Hacking.
 - d) Malware.

- 5 In the context of cyber threats, what does BEC stand for?
 - a) Business Email Compromise.
 - b) Business Encryption Code.
 - c) Business Exchange Chain.
 - d) Binary Exchange Component.

- 6 Which type of phishing involves cybercriminals sending deceptive emails or messages to obtain sensitive information?
 - a) Deceptive phishing.
 - b) Malware-based phishing.
 - c) Phone phishing.
 - d) Farming attack.

- 7 Which cyber threat involves directing users to a fraudulent website?
- a) Trojan Horse.
 - b) Pharming attack.
 - c) Ransomware.
 - d) Worm.
- 8 Which of the following is NOT a primary objective of opening Shell Companies in cyber frauds?
- a) Creating a current account.
 - b) Conducting legal trades.
 - c) Working with fintech companies.
 - d) Accepting or paying out proceeds of frauds.
- 9 What is the primary purpose of a firewall in cybersecurity?
- a) To update software.
 - b) To scan for malware.
 - c) To block unauthorized access.
 - d) To backup data.
- 10 In the year 2020, how many data breaches were reported in the United States?
- a) 895.
 - b) 1001.
 - c) 1,108.
 - d) 1,872.
- 11 What type of attack involves cybercriminals encrypting a victim's data and demanding a ransom for decryption?
- a) Phishing.
 - b) Malware.
 - c) DDoS.
 - d) Ransomware.
- 12 Which of the following threats involves long-term, highly sophisticated attacks often associated with nation-state actors?
- a) Advanced Persistent Threats (APTs).
 - b) Zero-Day Exploits.
 - c) Crypto jacking.
 - d) Supply Chain Attacks.

- 13 What does unauthorized access to electronic media refer to?
- a) Upgrading.
 - b) Networking.
 - c) Hacking.
 - d) Backing-up.
- 14 Which of the following was NOT a recommended strategy to prevent cyber threats?
- a) Regularly backup important data.
 - b) Limit user education.
 - c) Use multi-factor authentication.
 - d) Monitor bank and other financial transactions.
- 15 What refers to the practice of making false phone calls to trick individuals into revealing personal information or donating money?
- a) Web Phishing.
 - b) Email Phishing.
 - c) Phone Phishing or Voice Phishing.
 - d) Identity Theft.

Answers

- 1 b) Typical methods used by cybercriminals.
- 2 c) Purchase advanced software.
- 3 d) Ponzi scheme.
- 4 c) Hacking.
- 5 a) Business Email Compromise.
- 6 a) Deceptive phishing.
- 7 b) Pharming attack.
- 8 b) Conducting legal trades.
- 9 c) To block unauthorized access.
- 10 b) 1001.
- 11 d) Ransomware.
- 12 a) Advanced Persistent Threats (APTs).
- 13 c) Hacking.
- 14 b) Limit user education.
- 15 c) Phone Phishing or Voice Phishing.

**SELF-EXAMINATION QUESTIONS FOR PRACTICE**

- 1 What are the three primary elements that every modus operandi of cybercriminals will contain?
- 2 According to the study, during what period did cyberattacks become significantly more frequent, sometimes occurring multiple times in a single day?
- 3 Which type of cyberattack was the most frequent, accounting for 37% of all attacks between March 2020 and December 2021?
- 4 What does "BEC" stand for, and how does the FBI define it?
- 5 What was the primary method by which the Dani Data app scam defrauded its users?
- 6 Highlight the key differences between Viruses, Worms, and Trojan Horses.
- 7 Name at least three different phishing methods described in the content.
- 8 Why do cybercriminals create or utilize Shell Companies, especially in financial frauds?
- 9 Define "hacking" as mentioned in the context and provide an example of how unauthorized access might occur.
- 10 List two lessons learned from the Dani Data app scam to protect oneself from similar fraudulent schemes.

Chapter 4**Multiple Choice Questions (MCQ) for Practice**

- 1 What is Digital Forensics primarily concerned with?
 - a) Software development
 - b) Network monitoring
 - c) Identification and analysis of digital evidence
 - d) Database management

- 2 Which of the following is NOT a branch of the digital forensic investigation process?
 - a) Seizure
 - b) Reporting
 - c) Encryption
 - d) Acquisition

- 3 In which type of case is electronic discovery (eDiscovery) often involved?
 - a) Criminal cases
 - b) Civil cases
 - c) Tax fraud cases
 - d) Environmental cases

- 4 Which hashing functions are commonly used in the acquisition stage of digital forensics to verify data integrity?
 - a) AES and RSA
 - b) DES and ECC
 - c) SHA1 and MD5
 - d) WPA and WPA2

- 5 Why is the US Electronic Communications Privacy Act significant in digital forensics?
 - a) It promotes data encryption.
 - b) It restricts the sale of digital devices.
 - c) It places limitations on the ability to intercept and access evidence.
 - d) It facilitates easier data acquisition for forensics.

- 6 Which legislation governs the seizure of evidence by law enforcement in the United Kingdom?
 - a) The GDPR
 - b) The PACE act
 - c) The 1990 computer misuse act
 - d) The UK Digital Rights Act

- 7 What is one challenge faced by digital forensics due to technological advancements?
- a) Decreased data volumes
 - b) Simpler encryption
 - c) Rapid technological change
 - d) Reduced cloud storage
- 8 Which of the following is a type of data that a forensic analyst usually analyzes?
- a) Mobile applications
 - b) Chat logs
 - c) Software codes
 - d) Network routers
- 9 In the context of digital evidence, what does 'Authenticity' primarily deal with?
- a) Data encryption
 - b) Data volume
 - c) Confirming the integrity of information
 - d) Anti-forensics techniques
- 10 Which emerging technological area will require specialized forensic techniques due to its growth?
- a) Mainframe computing
 - b) Cloud Forensics
 - c) Optical storage
 - d) Analog devices
- 11 What technique is used by some to counteract forensic efforts?
- a) Data compression
 - b) Data migration
 - c) Data visualization
 - d) Anti-Forensics Techniques
- 12 Which branch of digital forensics is primarily concerned with data recovery from mobile devices like smartphones and tablets?
- a) Computer Forensics
 - b) Forensic Data Analysis
 - c) Mobile Device Forensics
 - d) Network Forensics
- 13 Which element of information security ensures that data or resources prevent improper and unauthorized changes?
- a) Confidentiality
 - b) Availability
 - c) Authenticity
 - d) Integrity

- 14 In which phase of the hacking cycle does an attacker gather preliminary data about the target without launching an actual attack?
- Gaining Access
 - Maintaining Access
 - Scanning
 - Reconnaissance
- 15 What distinguishes ethical hackers from malicious hackers?
- Ethical hackers use different tools.
 - Ethical hackers have permission to test systems, whereas malicious hackers do not.
 - Ethical hackers report vulnerabilities to the public.
 - Ethical hackers do not use their skills to identify vulnerabilities.

Answers

- c) Identification and analysis of digital evidence*
- c) Encryption*
- b) Civil cases*
- c) SHA1 and MD5*
- c) It places limitations on the ability to intercept and access evidence.*
- b) The PACE act*
- c) Rapid technological change*
- b) Chat logs*
- c) Confirming the integrity of information*
- b) Cloud Forensics*
- d) Anti-Forensics Techniques*
- c) Mobile Device Forensics*
- d) Integrity*
- d) Reconnaissance*
- b) Ethical hackers have permission to test systems, whereas malicious hackers do not.*

SELF-EXAMINATION QUESTIONS FOR PRACTICE



- What is digital forensics, and how has its scope evolved over time to include different types of digital devices?
- List the two primary legal scenarios where digital forensics is commonly employed and explain how electronic discovery (eDiscovery) plays a role in civil cases.
- Enumerate and describe the four main stages of the digital forensic investigation process.

- 4 How does the PACE act in the United Kingdom influence the seizure of evidence in digital forensic investigations?
- 5 Explain why the proliferation of Internet of Things (IoT) devices introduces complexities in digital forensic investigations.
- 6 Name two tools used in mobile device forensics and describe their primary functions.
- 7 What are the five branches of digital forensics and briefly explain the focus of mobile device forensics?
- 8 List three categories of challenges faced by digital forensics as classified by Eric Holder. Provide one example for each category.
- 9 Describe the five major elements of information security. How does authenticity differ from non-repudiation?
- 10 Define ethical hacking and explain its necessity in the context of an organization's cybersecurity.
- 11 What are the distinctions between Black Hats, White Hats, and Gray Hats? Provide a brief description of each.

Chapter 5**Multiple Choice Questions (MCQ) for Practice**

- 1 Which phase is the starting point of the digital forensic process?
 - a) Preservation
 - b) Documentation
 - c) Identification
 - d) Presentation

- 2 During which phase does the investigator decide the specific objectives of the investigation?
 - a) Case Assessment
 - b) Resource Allocation
 - c) Objective Definition
 - d) Risk Assessment

- 3 Digital evidence can include information from which of the following?
 - a) Traditional storage
 - b) Binary form
 - c) Analog devices
 - d) Paper archives

- 4 What is NOT a consideration in the identification phase?
 - a) Case Intake
 - b) Data Recovery
 - c) Legal and Ethical Considerations
 - d) Initial Documentation

- 5 In the analysis phase, what activity involves looking for specific files or types of files?
 - a) Data Recovery
 - b) Reporting
 - c) Examination
 - d) Analysis

- 6 What percentage of time do forensic investigation professionals dedicate to writing reports?
 - a) 10%-25%
 - b) 35%-50%
 - c) 50%-75%
 - d) 75%-90%

- 7 Which of the following is NOT an order of volatile data from most to least volatile for standard systems?
- a) Disk
 - b) Registers, cache
 - c) Routing table
 - d) Physical buttons
- 8 Which phase involves extracting and analysing digital Evidence?
- a) Collection
 - b) Preservation
 - c) Examination
 - d) Identification
- 9 If a device is ON during the evidence preservation process, what should you do with it?
- a) Turn it OFF
 - b) Keep it ON
 - c) Charge it
 - d) Immediately analyze its content
- 10 Why is the Chain of Custody important in digital forensics?
- a) To trace the device's manufacturing
 - b) To establish a timeline of device usage
 - c) To record the acquisition, custody, and transfers of evidence
 - d) To register the device for updates
- 11 What ensures that digital forensic results are reliable and admissible in court?
- a) Casual examination
 - b) Using any available software
 - c) Forensically sound manner
 - d) Taking frequent breaks
- 12 During which phase are the findings written up into a formal report?
- a) Preservation
 - b) Identification
 - c) Analysis
 - d) Reporting
- 13 What is the first step before writing a digital forensic report?
- a) Write the digital forensics report
 - b) Present the report to the court
 - c) Familiarize yourself with best practices
 - d) Automate your reporting

- 14 In Lab Investigation, what is the first activity?
- Preservation
 - Identification
 - Examination
 - Reporting
- 15 What do you do if you want to preserve the contents of the volatile memory of a computer?
- Shut down the computer
 - Hibernate it
 - Restart it
 - Disconnect from the internet

Answers

- c) Identification*
- c) Objective Definition*
- b) Binary form*
- b) Data Recovery*
- c) Examination*
- c) 50%-75%*
- d) Physical buttons*
- c) Examination*
- b) Keep it ON*
- c) To record the acquisition, custody, and transfers of evidence*
- c) Forensically sound manner*
- d) Reporting*
- c) Familiarize yourself with best practices*
- c) Examination*
- b) Hibernate it*



SELF-EXAMINATION QUESTIONS FOR PRACTICE

- What are the main objectives and components of the identification phase in the digital forensic process?
- Why the preservation of digital evidence is unique compared to traditional evidence, and what are some of the challenges faced?
- List the primary steps involved in the analysis phase and explain the importance of each.
- Why is documentation critical in both digital and physical forensic investigations?
- What are the key components that should be included in a comprehensive digital forensics report?

- 6 What are the main differences between the processes followed in a crime scene investigation and a lab investigation in digital forensics?
- 7 Describe the chain of custody and explain its importance in the digital forensic process.
- 8 What are the primary considerations and protocols when handling digital evidence to ensure its integrity?
- 9 What is meant by the "order of volatility" in digital forensics, and why is it important to understand this order?
- 10 Why is it essential to use legally obtained and reputable tools during the investigation process, and what are the potential implications of not doing so?

Chapter 6**Multiple Choice Questions (MCQ) for Practice**

- 1 What does this exposé primarily aim to address?
 - a) The history of Information Technology
 - b) The benefits of Information Technology
 - c) Information Technology crimes or cybercrimes
 - d) The financial implications of IT advancement

- 2 Which of the following is NOT mentioned as a type of Information Technology crime?
 - a) Hacking
 - b) Online shopping
 - c) Malware attacks
 - d) Identity theft

- 3 How many individuals were affected by the Equifax breach in 2017?
 - a) Over 200 million
 - b) Around 147 million
 - c) Less than 50 million
 - d) About 180 million

- 4 Which ransomware attack spread across over 150 countries?
 - a) BlackMirror
 - b) Spectre
 - c) Petya
 - d) WannaCry

- 5 What is the "Nigerian Prince" scam primarily known to exploit?
 - a) Technological loopholes
 - b) Human trust and vulnerability
 - c) Banking vulnerabilities
 - d) Cryptocurrency transactions

- 6 What was the primary purpose of Silk Road on the Dark Web?
 - a) A forum for tech enthusiasts
 - b) Facilitating illegal transactions
 - c) A hub for cryptocurrency exchange
 - d) An online library for academic research

- 7 Which international treaty seeks to harmonize national laws regarding cybercrime?
- a) Geneva Convention
 - b) Paris Agreement
 - c) Budapest Convention on Cybercrime
 - d) Rome Statute
- 8 What is the primary role of the United States' CISA?
- a) Regulating internet content
 - b) Managing IT infrastructures
 - c) Combating and countering cyber threats
 - d) Overseeing telecommunication services
- 9 Which approach assumes that every access request, internal or external, must be verified?
- a) Open Door Policy
 - b) Universal Trust
 - c) Zero Trust model
 - d) Absolute Verification
- 10 Which of the following is a recommended method to combat cybercrimes?
- a) Discouraging public from using the internet
 - b) Raising public awareness about cybercrimes
 - c) Limiting international collaborations on cyber threats
 - d) Allowing unrestricted access to dark web for research
- 11 Which act serves as a central piece of legislation in India's response to cybercrimes?
- a) Digital Protection Act, 2005
 - b) Cybersecurity Framework, 1995
 - c) Information Technology Act, 2000
 - d) Electronic Transaction Act, 2008
- 12 Which of the following was NOT mentioned as an emerging threat in the context of evolving IT crimes?
- a) Quantum Computing
 - b) AI-assisted cyber attacks
 - c) Ransomware as a Service
 - d) Cloud Bursting
- 13 What potential does quantum computing have in the realm of cybersecurity?
- a) Only to strengthen encryption methods.
 - b) Only to break existing cryptographic methods.
 - c) Both strengthen encryption and break existing cryptographic methods.
 - d) None of the above.

- 14 Which case highlighted the challenge of jurisdiction in cross-border cybercrime?
- Operation Aurora
 - The Kevin Mitnick Odyssey
 - Gary McKinnon Saga
 - The Deep Web Enigma
- 15 SEBI's guidelines emphasized which of the following for Market Infrastructure Institutions (MIIs)?
- Promoting regular vulnerability scanning.
 - Focusing only on offline data backups.
 - Encouraging a passive approach to implementing cybersecurity guidelines.
 - Establishing a limited cybersecurity framework.

Answers

- c) Information Technology crimes or cybercrimes*
- b) Online shopping*
- b) Around 147 million*
- d) WannaCry*
- b) Human trust and vulnerability*
- b) Facilitating illegal transactions*
- c) Budapest Convention on Cybercrime*
- c) Combating and countering cyber threats*
- c) Zero Trust model*
- b) Raising public awareness about cybercrime*
- c) Information Technology Act, 2000*
- d) Cloud Bursting*
- c) Both strengthen encryption and break existing cryptographic methods.*
- c) Gary McKinnon Saga*
- a) Promoting regular vulnerability scanning.*



SELF-EXAMINATION QUESTIONS FOR PRACTICE

- What are the main objectives of the Information Technology (IT) Act, 2000, in India, and how has it evolved to address the concerns of cybercrimes?
- List and briefly describe five different types of Information Technology crimes mentioned in the content.
- Discuss the implications of the Equifax Breach and its significance in the realm of cybercrimes.
- How does the IT Act, 2000, ensure the authenticity of online transactions in India?

- 5 What responsibilities do companies have concerning data protection under the amended IT Act, and what are the potential repercussions for negligence?
- 6 Highlight three recommendations for India to enhance its fight against IT crimes in the future based on the content provided.
- 7 How do Artificial Intelligence (AI) and Machine Learning (ML) algorithms contribute to the detection and mitigation of cyber threats in real-time? Provide examples.
- 8 Discuss the implications of quantum computing on cybersecurity, highlighting both its potential benefits and threats to digital security.
- 9 Describe the challenges and ethical considerations that arise when integrating AI and machine learning into cybersecurity practices. Why is it essential to ensure the ethical use of data and unbiased algorithms?
- 10 Explain the importance of global cooperation in the realm of cybersecurity. How do international accords and collaborations, such as the Paris Call for Trust and Security in Cyberspace, contribute to enhancing global cybersecurity measures?

Chapter 7**Multiple Choice Questions (MCQ) for Practice**

- 1 What does OSINT stand for?
 - a) Open-Source Interface Technology
 - b) Open-Source Internal Transfer
 - c) Open-Source Intelligence
 - d) Official Source Interface Technology

- 2 Which tool is primarily used for gathering metadata from documents connected to an organization?
 - a) Censys
 - b) ThreatCrowd
 - c) FOCA
 - d) Recon-ng

- 3 What is the main function of the Wayback Machine?
 - a) Analysing SSL Certificates
 - b) Identifying Vulnerable Devices
 - c) Archiving screenshots of websites
 - d) Identifying network shares

- 4 Which of the following is NOT a feature of Cellebrite UFED Physical Analyzer?
 - a) Malware Detection
 - b) SQLite databases viewer
 - c) Phishing Site Detection
 - d) Passcode recovery attacks

- 5 Which tool is a search engine for internet-connected devices and networks?
 - a) Spider-Foot
 - b) Netcraft
 - c) Censys
 - d) The Harvester

- 6 Which OSINT tool specializes in web reconnaissance?
 - a) Wayback Machine
 - b) FOCA
 - c) Recon-ng
 - d) Censys

- 7 What information does Netcraft provide regarding SSL/TLS?
- a) Password Recovery
 - b) Certificate Analysis
 - c) Website History
 - d) Phishing Site Detection
- 8 Which tool aids in detecting and tracking phishing sites?
- a) FOCA
 - b) Netcraft
 - c) Censys
 - d) Spider-Foot
- 9 Recon-ng is open-source and is used by professionals primarily for?
- a) SSL/TLS Certificate Analysis
 - b) Information gathering and reconnaissance
 - c) Digital Footprint Analysis
 - d) Metadata Analysis
- 10 Which tool helps with network reconnaissance by identifying open ports, protocols, and SSL/TLS certificate information?
- a) Netcraft
 - b) Recon-ng
 - c) Censys
 - d) ThreatCrowd
- 11 Which of the following tools aids in understanding the security posture of a target entity by aggregating information from various sources?
- a) ThreatCrowd
 - b) Spider-Foot
 - c) The Harvester
 - d) Cellebrite UFED Physical Analyzer
- 12 Why is ethical consideration crucial in OSINT activities?
- a) To ensure maximum data extraction
 - b) To maintain the speed of data collection
 - c) To respect individuals' privacy rights
 - d) To increase the accuracy of data
- 13 In the context of digital forensics, what does the term 'IoC' stand for?
- a) Input of Command
 - b) Internet of Connectivity
 - c) Indicators of Compromise
 - d) Integration of Code

- 14 Which tool provides historical records of websites showing how a site has evolved over time?
- Spider-Foot
 - Recon-ng
 - Wayback Machine
 - FOCA
- 15 For which purpose is Maltego primarily used?
- Archiving screenshots of websites
 - Vulnerability Assessment
 - Visualizing Data Relationships
 - Analysing SSL Certificates

Answers

- c) Open-Source Intelligence*
- c) FOCA*
- c) Archiving screenshots of websites*
- c) Phishing Site Detection*
- c) Censys*
- c) Recon-ng*
- b) Certificate Analysis*
- b) Netcraft*
- b) Information gathering and reconnaissance*
- c) Censys*
- a) ThreatCrowd*
- c) To respect individuals' privacy rights*
- c) Indicators of Compromise*
- c) Wayback Machine*
- c) Visualizing Data Relationships*

SELF-EXAMINATION QUESTIONS FOR PRACTICE



- What does OSINT stand for and what is its primary role in cyber forensics investigations?
- Describe the functionalities of Cellebrite UFED Physical Analyzer in the context of digital forensics. What are some of its notable features for iOS, Android, and BlackBerry devices?
- Discuss the significance and capabilities of Magnet AXIOM in digital investigations, highlighting its two main components: AXIOM Process and AXIOM Examine.
- Explain how the Wayback Machine functions. How can it be utilized in digital forensics?

- 5 Outline the main features and applications of FOCA (Fingerprinting Organizations with Collected Archives) in gathering information from documents and files.
- 6 How does Censys assist digital forensics investigators in uncovering vulnerabilities? Discuss its main applications in the realm of cyber forensics.
- 7 Describe the functionalities and applications of SpiderFoot in comprehensive data gathering. What are its key benefits in the context of digital forensics?
- 8 Discuss the main capabilities of Recon-ng as a web reconnaissance framework. How does it assist in gathering OSINT data and automating data analysis?
- 9 Highlight the importance of ethical and legal considerations in OSINT. Why is respecting privacy and adhering to legal frameworks vital in OSINT activities?
- 10 Considering the evolving cyber landscape, explain the importance of adapting to technologic advancements and the role of lifelong learning in the domain of OSINT and digital forensics.

Chapter 8**Multiple Choice Questions (MCQ) for Practice**

- 1 What is digital forensics primarily used for?
 - a) Identifying market trends
 - b) Collecting and preserving digital evidence
 - c) Analysing customer behaviour
 - d) Monitoring employee productivity

- 2 Which discipline focuses on ensuring the accuracy and reliability of financial records?
 - a) Digital forensics
 - b) Auditing
 - c) Forensic accounting
 - d) Data mining

- 3 What is the main driving force behind the convergence of digital forensics, auditing, and forensic accounting?
 - a) Increasing globalization
 - b) Growth in cryptocurrency usage
 - c) The digitization of financial records
 - d) Advances in AI technology

- 4 How can digital evidence be used in financial investigations?
 - a) To identify customer segments
 - b) To track email communications
 - c) To create financial records
 - d) To develop marketing strategies

- 5 What is the purpose of ratio analysis in financial data analysis?
 - a) To compare financial data points and assess a company's financial health
 - b) To identify fraudulent transactions
 - c) To recover deleted files
 - d) To trace the movement of money

- 6 Which software can be used to identify fraudulent transactions in financial data?
 - a) Data mining software
 - b) Data visualization software
 - c) Fraud detection software
 - d) Data encryption software

- 7 What is the primary advantage of financial data analysis?
- a) Increased data complexity
 - b) Enhanced fraud detection
 - c) Limited data availability
 - d) Reduced decision-making effectiveness
- 8 Which of the following is a limitation of financial data analysis?
- a) Accurate and complete data
 - b) Lack of ethical considerations
 - c) Overfitting of models
 - d) Unbiased analysis
- 9 What is a potential ethical concern in the context of data privacy?
- a) Protecting individual rights
 - b) Maximizing data collection
 - c) Ignoring data quality
 - d) Overfitting data models
- 10 How can chartered accountants protect data privacy and ethics?
- a) By using data for any purpose without consent
 - b) By deleting data as soon as it is collected
 - c) By collecting minimal data and anonymizing it
 - d) By sharing data with unauthorized parties
- 11 What is a key strategy for maintaining data integrity?
- a) Collecting excessive data
 - b) Using inconsistent encryption methods
 - c) Implementing access controls
 - d) Avoiding regular audits
- 12 How can chartered accountants stay up-to-date on data privacy and ethics?
- a) By ignoring industry publications
 - b) By not attending any training or workshops
 - c) By avoiding collaboration with other professionals
 - d) By attending training and workshops, and reading industry publications
- 13 Which global regulation mandates strict data handling rules?
- a) Sarbanes-Oxley Act (SOX)
 - b) European Union General Data Protection Regulation (GDPR)
 - c) California Consumer Privacy Act (CCPA)
 - d) International Financial Reporting Standards (IFRS)

- 14 What is a benefit of using a holistic approach to data privacy and ethics?
- a) Maximizing data collection
 - b) Minimizing individual rights
 - c) Protecting individual rights, building trust, and mitigating risks
 - d) Ignoring data protection regulations

- 15 What is a primary role of independent ethical review boards in sensitive cases?
- a) Assessing financial transactions
 - b) Reviewing marketing strategies
 - c) Evaluating data privacy policies
 - d) Assessing methods and guiding ethical decisions

Answers

- 1 *b) Collecting and preserving digital evidence*
- 2 *b) Auditing*
- 3 *c) The digitization of financial records*
- 4 *b) To track email communications*
- 5 *a) To compare financial data points and assess a company's financial health*
- 6 *c) Fraud detection software*
- 7 *b) Enhanced fraud detection*
- 8 *c) Overfitting of models*
- 9 *a) Protecting individual rights*
- 10 *c) By collecting minimal data and anonymizing it*
- 11 *c) Implementing access controls*
- 12 *d) By attending training and workshops, and reading industry publications*
- 13 *b) European Union General Data Protection Regulation (GDPR)*
- 14 *c) Protecting individual rights, building trust, and mitigating risks*
- 15 *d) Assessing methods and guiding ethical decisions*



SELF-EXAMINATION QUESTIONS FOR PRACTICE

- 1 What is the convergence of digital forensics, auditing, and forensic accounting, and why is it important in today's financial landscape?
- 2 How does digital evidence play a crucial role in detecting financial anomalies and fraud in modern financial investigations?
- 3 What specialized skills are essential for modern financial investigators, and how do they contribute to effective financial crime detection?
- 4 What are the advantages and limitations of using financial data analysis in financial investigations, and how can it benefit organizations?

- 5 What are some practical digital tools and software modules used in financial data analysis, and how do they aid in investigations?
- 6 How can chartered accountants ensure compliance with data protection regulations, especially in a complex global data privacy landscape?
- 7 What strategies can be employed to balance investigative needs with ethical considerations, particularly regarding privacy and informed consent?
- 8 How does transparency contribute to ethical financial investigations, and what role does comprehensive documentation play in ensuring transparency?
- 9 What ethical principles should chartered accountants uphold when handling data, and what are some strategies for maintaining ethical data practices?
- 10 What challenges and trends in data privacy should chartered accountants be aware of, and how can they adapt their practices to address these challenges effectively?



UNIT

3

Robotic
Process
Automation

CHAPTER 1

TECHNOLOGY AND ITS EFFECTIVE USE IN FINANCE & ACCOUNTS

1.1 Evolution of Accounts & Finance function by adopting technologies over time

Manual accounting was the only method of accounting available until recent times. Businesses had to hire a full-time or part-time accountant or bookkeeper, for this purpose. They would manually record transactions, generate books and ledgers, and prepare financial statements. They had to do all accounting work manually on paper and books.



It would take a lot of time and resources to generate and trace documents and records from the record rooms. Since everything was manual, the system was ineffective from a control perspective as the task of an accountant (popularly known as Munim Ji) would be only to record the transactions without putting much thrust on verification, validation, and control. Accounting graduates were in high demand as they were the only ones to understand the culture of Financial Registers, Books, and Ledgers.

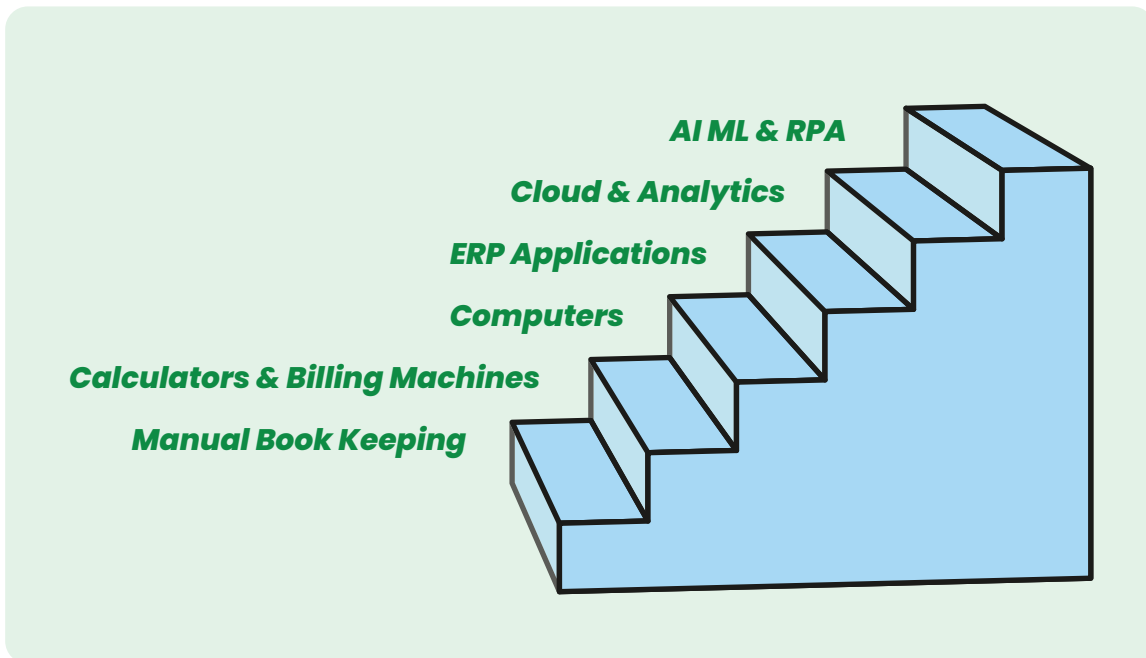
The accounting process later moved to computerized systems like billing machines. As we read above, these machines resembled typewriters and calculators and people used them in stores. They performed tasks like calculating net totals, deducting discounts, recording billing information, etc. Even tools like calculators and billing machines were of great help to accountants in reducing their tasks, calculating balances, and balancing records.

With the introduction of newer technology, modern computerized systems made accounting easier. They enabled users to enter accounting data in real time. Apart from basic outcomes, these technological innovations helped record sophisticated transactions as well.

With the availability of Enterprise Resource Planning (ERP) software in the 1990s businesses realized the value of having integrated applications, which would automatically integrate

accounting with the business of Sales, Purchases, Inventory, Manufacturing operations, Projects, and Human Resources. ERP helped organizations focus on business and its growth rather than worry about transaction processing. ERP is now part of every organization, without which businesses don't start. The advantages of ERP for business included:

- 1 One business transaction processing system integrated with business operations
- 2 One version of truth, no mismatch of data
- 3 Control over business transactions and functions
- 4 Instantaneous availability of information for better decision-making



ERP brought its own set of challenges as well. The biggest of these challenges was

- 1 The increased cost of IT operations, as organizations were not used to investing in IT Infrastructure, hence with the adoption of ERP the organization needed computers for all and high-cost Infrastructure
- 2 Change management, employees working in organizations were not aware of the capability of ERP and started to feel threatened for their jobs
- 3 Data entry, ERP being an integrated platform increased data entry task in ERP

Slowly, the challenges were overcome by the benefits of deploying ERP. Nowadays, almost all businesses have ERP setups for their organization. The selection of ERP depends upon the nature and complexity of businesses.

CHAPTER 2

INTRODUCTION TO ROBOTIC PROCESS AUTOMATION (RPA)

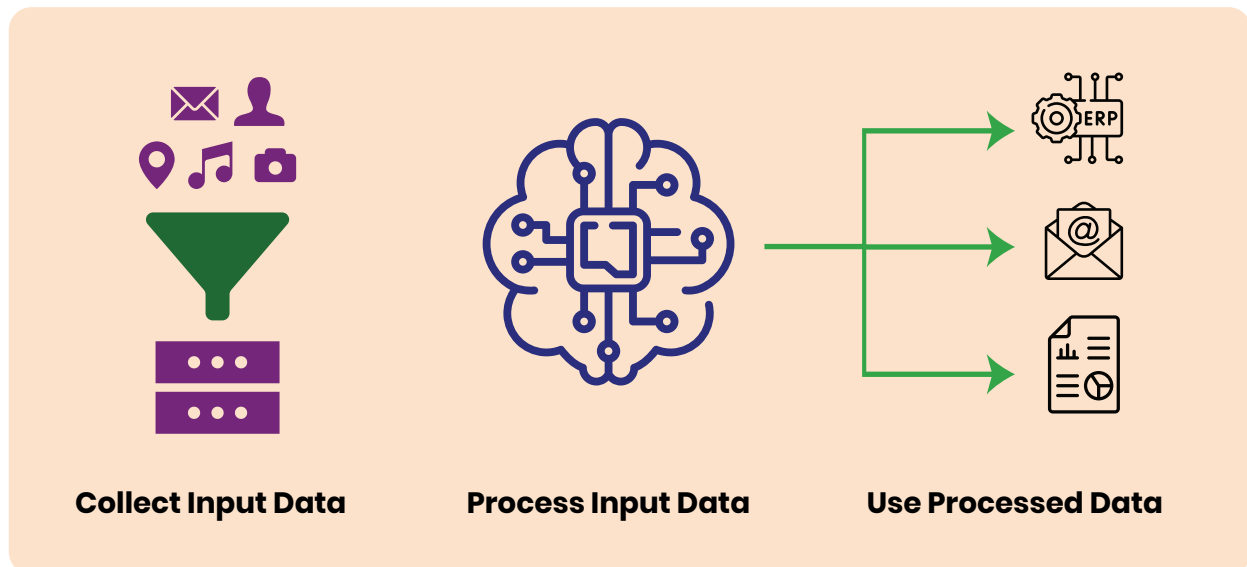
2.1 WHAT IS RPA?

RPA can be a pretty slippery term, in a way that the more one tries to understand and more it broadens its hemisphere. The word “Robotic” may sound like a physically shaped strong and bulky BOT but it is all about software, with no physical shape or form. Like any other software “Robotic” also supports human efforts by automating human activities in an enterprise (mostly activities in clerical and administrative functions).

Even the word “Process” can also be misnomer, a better alternative would be “task”, which is what RPA aims to automate. A combination of such “tasks” adds up to a process.

So, RPA as a process can be understood as a technological advancement, which is a combination of a Platform, Artificial Intelligence, and Machine Learning, developed to form a software product called “Robotic”. It is then programmed/ trained to complement human efforts by automating mundane activities done by humans. These activities include data entry, computation using fixed formulae, etc.

RPA can be better understood as a Digital Worker trained to tasks performed by humans with no or minimal value. It primarily performs below functions (Refer to Figure 1 below):



- 1 **Collection of Inputs:** RPA can be trained to collect data as input from any digital source including,
 - a PDF copies of documents – e.g. A PDF copy of Vendor Invoices
 - b Images of documents – e.g., Images of Invoices, designs, etc
 - c Voice recordings – e.g., Audio recordings and speech
 - d Texts & Posts – e.g., Social Media posts, Queries & Complaints.
 - e Web portals – e.g., Bank portals, Stock exchange portals, etc
 - f Structured or unstructured datasets – eg. ERP database or emails and other documents

- 2 **Processing of raw data collected:** RPA has a strong processing engine, coupled with Artificial Intelligence and Machine Learning, it can process volumes of data with unmatched speed and without any errors. The processing capabilities include:
 - a Complex calculations on raw data derived from single of multiple sources.
 - b Formatting of raw data to be used in further processing.
 - c Comparing raw data obtained from multiple sources and highlight anomalies.

- 3 **Entering/ Presenting/ publishing the data in the Target application:** RPA can use the processed data for variety of ways including:
 - a Enter the data in any Target application like Tally, SAP etc.
 - b Filling of forms on web portals like GST portals, Bank portals
 - c Sending the formatted data to the target users through mails or any other medium of communication
 - d Engaging with Users and respond to their queries in the form of chatbots.
 - e Publish reports and dashboards based on the processed data to the target users.

In simple words RPA can perform below with ease, more efficiently and effectively

- 1 Cut & paste information from one application to another

- 2 Opening of a website and login with the credentials

- 3 Opening of e-mails and downloading and reading attachments

- 4 Read and write entries in database

- 5 Extraction of information from any forms and documents

- 6 Calculations and workflows for verification and approvals

2.2 WHY RPA?

The world is full of opportunities and has limited resources including employable people. Technology companies, across the globe, are always working to develop technology to maximize the usage of such scarce resources. RPA is the latest technology, which can work alongside humans to free them from mundane and repetitive tasks so that humans can focus on more important tasks without worrying about mundane tasks. RPA's versatility is proving to be handy and is being recognized.

As per the study by Forbes, humans generate more digital data in last every five years than ever before. With the volume of data being generated and consumed each day, it's just impossible for humans to track the data and its usefulness due to the sheer volume and source. No matter how many employees one engages for the job, an RPA can do such a task without any strain.

RPA was developed to reduce dependency on such mundane tasks so that humans can focus efforts and energy on value-added tasks for promoting business interests. Tasks such as mentioned below:

- 1 Research and Development
- 2 Taking Decisions for actions with no significant historical precedence
- 3 Innovative ideas
- 4 Customer connects and service
- 5 Certifications



2.3 THE BENEFITS OF RPA



RPA does not have any form of physical robot. It mimics a human work by interacting with applications in a similar way that a human does. It also allows for interpreting existing applications, activating responses, controlling data, and communicating with other digital systems. RPA Solutions can be enhanced with machine learning and Artificial Intelligence.

RPA is used for the benefit of different domains:

- **Finance- RPA in Finance can help by automating**
 - Vendor Invoice Processing
 - Bank Reconciliation
 - Receiving and Sending e-mails with documents and reminders

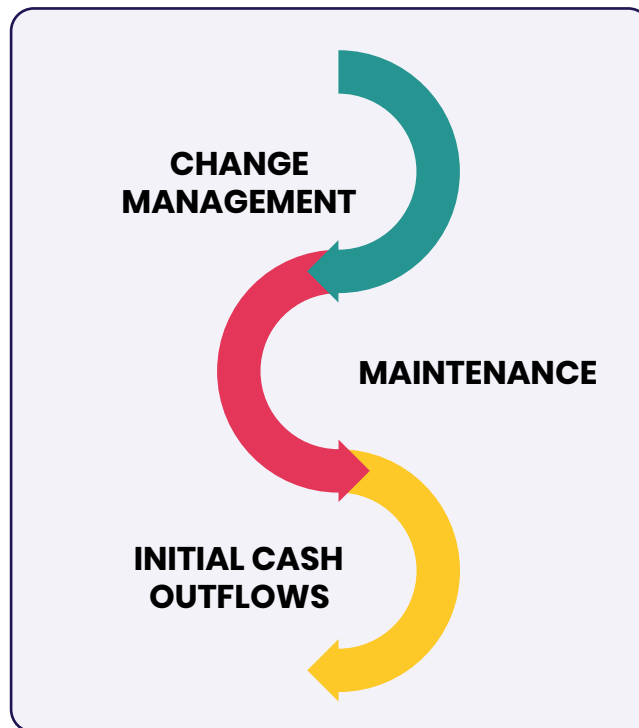
- **Supply Chain- RPA in Supply Chain helps by automating**
 - Gathering data from the World Wide Web and analyzing business patterns
 - Internal adjustments to avoid potential disruptions and bottlenecks
 - Effective planning and execution of business
- **Human Resources- RPA in Human Resources can help by automating**
 - New employee onboarding and joining formalities
 - Payroll Processing
 - Chatbots for queries and clarifications
 - Employee productivity analysis

There are a lot of benefits of using RPA in real-life scenarios. Quality and quantum of benefits will vary from business to business, however, some of the common benefits due to RPA are:

- **COST SAVINGS-** A major benefit of RPA is a quick reduction in costs associated with the operations. By automating tasks cost savings of anything between 30% - 50% is realized immediately. This becomes the major factor in the adoption of RPA
- **EMPLOYEE PRODUCTIVITY-** RPA supplements human efforts of doing work more effectively and efficiently, thereby freeing them to focus on other revenue-generating activities like customer connection, and relation management. Spending time on revenue-generating activities rather than mundane activities has an impact on growing revenue.
- **QUALITY & ACCURACY-** RPA is deployed to automate processes, which have a high probability of human errors when processed manually. RPA is always consistent, and reliable and never complains when expected to overwork tirelessly. These qualities of RPA reduce the chances of re-work and enhance quality. The most important point is that RPA works on a set of rules and never deviates from rules thereby producing 100% accuracy.
- **SCALABLE-** RPA is a piece of software with no emotions, it can be easily adjusted for business changes due to seasonality. It can easily be scaled up and down as per the requirements of the business without any complaints.
- **CONTROL-** Companies prefer to outsource such tasks to external partners, which leads to compromise in quality, inefficiency, and risk of losing confidential data to competitors. RPA provides a solution where the work and data remain in-house with no such challenges of data compromise or inefficiency.

2.4 CHALLENGES IN RPA

The world is full of opportunities and has limited resources including employable people. Technology companies, across the globe, are always working to develop technology to maximize the usage of such scarce resources. RPA is the latest technology, which can work alongside humans to free them from mundane and repetitive tasks so that humans can focus on more important tasks without worrying about mundane tasks. RPA's versatility is proving to be handy and is being recognized.

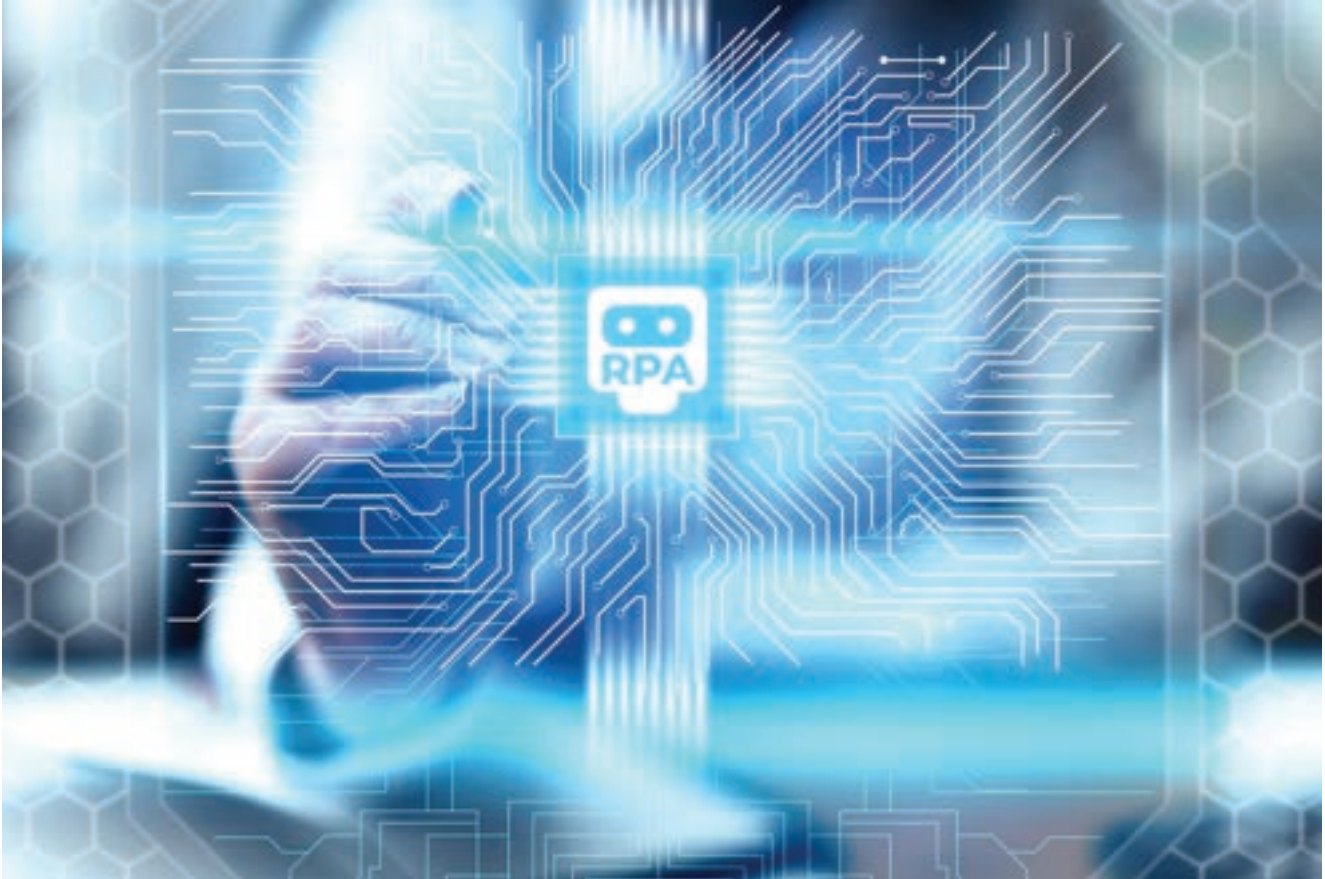


Though RPA has significant benefits it comes with its own set of challenges. One has to be mindful of these challenges before adopting RPA across functions. Some of the critical challenges include:

- **CHANGE MANAGEMENT-** The adoption of RPA is generally conceived as a replacement of people with Bots, hence the fear of job loss, which results in potential resistance by employees to its adoption. The decisive success factor for automation is therefore communication as part of Change Management.
- **RECURRING MAINTENANCE-** RPA needs to be maintained for changes in the business environment and changes in Source and Target data structures.
- **HIGH INITIAL COSTS-** Setting up RPA has costs of both software, associated hardware, and initial setup. One has to be watchful of these costs before adopting RPA for the functions.

CHAPTER 3

IMPACT OF RPA



Technology will continue to transform society at a rapid pace, and accounting is one of those areas that has adapted itself to these innovative changes. New technologies are being innovated, which is able to mimic human activity, taking on repetitive work more rapidly and accurately than people can. Overview of Robotic Process Automation (RPA) in accounting will change the ways the profession operates, with a specific focus on the field of revenue audits. With the implementation of RPA, several accounting tasks that are usually repetitive and time-consuming will be at ease. Automation of tasks by RPA, such as collection of data, management of risks, function of accounts payable/ receivable, and many more. RPA enhances the ability of employees by simplifying complicated human work. RPA becomes more effective if it is used to make processes more efficient so that manpower can be utilized for performing value-added work. While deploying RPA in accounting it should be noticed that the automated processes may have minor errors, however, such errors will be identified and rectified never to recur again but initially, accountants must recheck the data to be sure that it has accuracy.

4.1 ROBOTIC PROCESS AUTOMATION (RPA)

RPA takes help from the end-users to configure/ train a software robot and also to integrate existing applications that record, store, manipulate data, execute transactions, and communicate with other systems. RPA is a technology-driven solution, which can automate rule-dependent and standardized functions using small programs called scripts. The use of RPA is become more popular in recent years, several software robots are being easily trained and programmed to perform rule-related, repetitive, high-volume works by replicating human actions when accessing multiple systems, documents, and applications.

The robots can do work with the help of a user interface in the same manner a human does eliminating the requirement to modify applications (e.g., ERP, software warehouse, accounting, and payroll) or the important information technology infrastructure. Each robot operation is logged and tracked to meet audit needs and ensure data integrity.

Human involvement is very necessary only to the extent of initial set-up as the robot, today is capable of extracting data from structured and unstructured formats of data. For instance, scanned documents and even images captured from mobile devices. There may be some tasks, that are difficult to automate due to the involvement of integration of multiple applications not built on a new-age platform. For instance, some organizations still use COBOL and FOXPRO applications.

4.2 RPA IN ACCOUNTING

RPA has garnered huge interest from several accounting and outsourcing organizations, specifically related to the tasks of taxation, advisory, and assurance services. For instance, a significant portion of tax activities, like the calculation of book tax, transfer pricing, variations, and the preparation of tax returns, have been automated due to the adoption of technology in accounting. RPA is also presented to clients as an advisory product and service. The RPA software has been vastly applied for tax and advisory works.

The main objective of RPA in accounting is the management of repetitive functions and enhanced productivity, efficiency (minimal human errors) as well and cost-effectiveness. Accounting divisions are a perfect match for RPA because they consist of repetitive work that is mundane, tedious, and demands a lot of attention to understand in detail. Accounting mechanisms like Accounts Payable and Accounts Receivable are crucial for a firm's end-to-end functionality.

- **Use Cases of RPA in Accounting**

The management of a business's accounts often needs a diverse set of software systems, because a single package cannot take care of all the necessary work. That separation of systems often results in a massive amount of time-consuming and recurring work, which is solely suitable for automation through RPA. Let's have a look at some of the use cases of robotic process automation in accounting.

- **Integrating Policies, Procedures & Systems**

It's important to have integrated policies, procedures, and systems before using RPA in the accounting field. One has to be careful about the tasks to be automated and the result, if the result is not verified and all the scenarios are not tested, with the speed of RPA, it can generate a huge volume of inaccurate transactions by the time these transactions are noticed and identified. Rectifying these transactions can be difficult. The hidden part of RPA is that it extends across the entire process and automates those manual, error-prone procedures in the last mile of accounts, which drastically minimizes the risk while delivering dependable data.

During the financial close, balances are required to get validated, records should be consolidated, journal entries must be adjusted, financial data is taken for disclosure, and financial statements need to be prepared. There are high chances of risk for error in these works, and that's the time the hidden value of RPA gets available.

- **Reducing Cost and Enhanced Efficiency**

According to Gartner, "The last mile of Finance is ripe for cost reduction and efficiencies. While costs and resource consumption can be reduced by automating these processes, the bigger financial impact is in preventing the fallout from penalties, fines, lawsuits, and valuation that result from inaccurate filing of financial statements."

With RPA, huge volumes of data can be processed at an unimaginable speed while offering a high level of accuracy and giving visibility into the tiniest of details, irrespective of business segment or geographical spread. Though there is unquestionably immense value in the reduction of the close timeline that gives analytics time, RPA gives unparalleled accuracy, visibility, and elimination of risk. According to the Institute for RPA, "RPA solutions can help organizations save 25-40 percent in labor costs."

While RPA also offers Return on Investment (ROI) across the complete procedure, a few ROIs are simpler to measure when compared to others. It is easy to compare ROI on the reduction of FTE hours on mundane work and maximization in mere efficiency but the greater impact of RPA is in its elimination of negative financial aspects, which include the capability to avoid mistakes before they are made or automatically attach documentation to proactively ignore the audit fees.



- **Reconciliations**

A lot of accounting effort is used to explain open things and flush out the deviations plug (imbalances) continuously in the month and not at the end which can make it late for balance confirmation, finalizing accurate balances of payable and receivables forecasting, and financial reporting processes. If these types of transactions are not correctly accounted for, any out-of-balance accounts can impact the financial statements, creating compliance problems and risk of restatement, where regulatory agencies may impose huge fines and penalties. Such restatements can also hurt the investors' confidence, which may reflect in the process of the organization's share price.

The Reconciliation Hub embeds configurable matching ways to operate transaction reconciliations based on the RPA in accounting tolerance levels, identifying exceptions automatically that are best for managing the growth of transaction volumes. It also enables companies to centralize such reconciliations' documentation, transactional insights, agreements, and costs while acting as an ERP-agnostic connective tissue between different entities.

- **Financial Planning & Forecasting**

The process of Planning becomes very difficult if there is no availability of accurate data.

The actuals are the performance for the business, by comparing these actual figures against budgeted figures, and this is also where they can extract the forecasted figures for the business segment. The variables, in which the business segment operates are changing rapidly in the current market environment, the modern accounting processes get adjusted accordingly. In the traditional environment, finance often spends most of its time painfully getting the numbers right with manual, spreadsheet-based processes.

According to EY, “finance teams spend the majority of their time working on the financial works itself, which means the business has to wait until after the period-end for information.”

The technology in accounting helps to transfer the nature of Finance’s work from canned after-the-fact (post-mortem jobs) reports to answer questions to the business with better, quicker insights. RPA is a powerful value driver for data analytics initiatives in an ever-emerging digital landscape, working in tandem with integration objects to integrate the technology ecosystem and put data or results into downstream systems. By integrating systems and data in this way, the efficiency provides more time for accounting professionals to analyze results and look deeper at trends to better support agile forecasting and scenario planning.

- **Advantages of RPA in Accounting**

Robotic process automation in accounting bots meets with legacy systems and applications, implying that they can bring about the desired change in business without disrupting the prevailing business policies and practices. Compared with several various traditional IT solutions and accounting software, RPA is applied in very little time and most affordable prices.

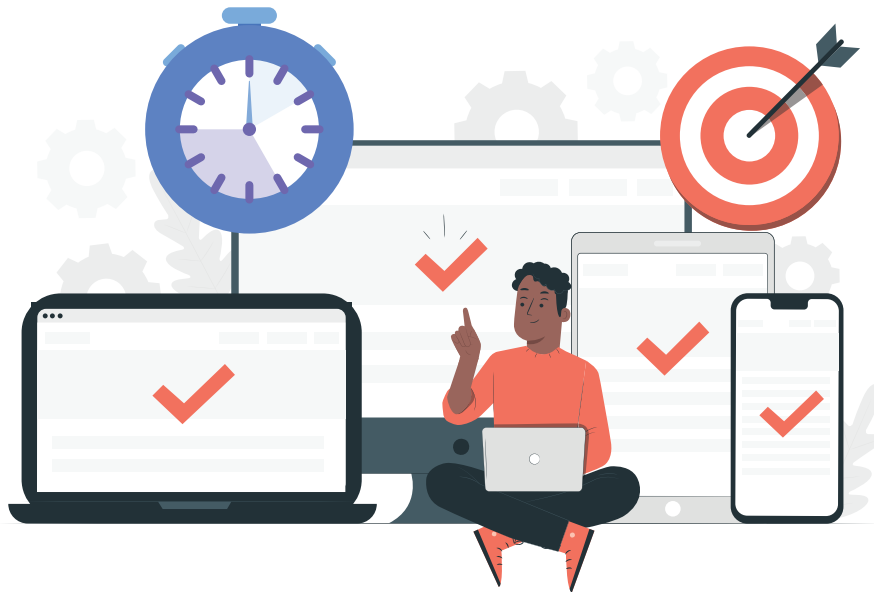
RPA possesses huge potential; it provides better efficiency. Let’s have a look at a few advantages of RPA in accounting:

- **Time-saving by bringing in efficiency**

RPA automates a lot of activities and saves a lot of accountants’ time. An accountant then spends more time focusing on work that brings greater value to the growth of the business. RPA gives a quicker turnover of documents for approval, resulting in rapid clearing of suppliers’ invoices.

- **Maximum accuracy**

RPA automates a lot of activities and saves a lot of accountants’ time. An accountant then spends more time focusing on work that brings greater value to the growth of the business. RPA gives a quicker turnover of documents for approval, resulting in rapid clearing of suppliers’ invoices.



- **Improves productivity**

By automating mundane accounting processes, a lot of time will be saved for accounting professionals. As a result, they get a lot of time to focus on other value-added tasks, which will enhance their productivity resulting in a reduction in overall costs of operation. They can use their time and skills to do other essential tasks to serve clients the best.

- **Better customer experience**

The RPA has helped to move the focus of accounting professionals more on enhancing the quality of work, which increases overall customer satisfaction resulting in business performance and revenues. Deploying an RPA system gives firms more time to do research, customer service, get a competitive advantage, and scale operations while decreasing the cost. It also enables a top level of customer service and more strategic work for the team.

4.3 THE FUTURE OF ROBOTIC PROCESS AUTOMATION

There is a fast adoption of RPA in several organizations globally, less than one-third of adopters use the technology in accounting and financial reporting. The RPA application is growing in popularity across all business functions. If the business adopted the RPA, one can expect RPA to be adopted in other departments – and soon.

Combining Artificial Intelligence (AI) with RPA has made RPA even more effective and relevant than ever before. Intelligent automation brings a higher value to technology than just RPA. For instance, RPA can easily fill out a tax report, but if the tax form changes; its rules must be reprogrammed. Adopting AI to read a tax form and change RPA rules depending on its discoveries will give a whole new path to accounting automation.



TO CONCLUDE

Robotic process automation in accounting changes the role of finance to more strategic than tactical and transactional. It gives accounting professionals more time and visibility into business performance to strive for continuous improvement. Several organizations have frequent process reviews that will seek ways to fix them. Process automation stays and sustains consistency in execution, which translates into fewer process problems to deal with. A well-designed RPA system makes it straightforward to make adjustments to the overall processes.

RPA frees individuals from mundane activities to turn their focus and attention to the value-adding tasks that benefit their professional skills, training, and experience. It also ensures finance executives use the profits efficiently to concentrate on filling a strategic role in their organization by offering timely and insightful details that are rapidly transforming the tech landscape and advancing in the accounting changing initiatives.

UNIT

4

**ORACLE
FUSION ERP**

CHAPTER 1

P2P CYCLE AUDIT

1.1 WHY P2P CYCLE AUDIT IS IMPORTANT

Procurement is the most complex process for the businesses as it involves a number of operations and incurring huge amount of outflow of money from the business. It's a challenge for the organization from the very beginning from supplier selection to the final payment, as it involves many processes and different persons are handling the process. Still it is important to audit the entire purchasing flows even ERP solutions offers process automation.

Key reasons why P2P process needs an audit:

- 1 Purchases from unauthorized suppliers
- 2 Chances of non-Purchase orders
- 3 Invoices which are not matched to PO or GRN
- 4 Payments without delivery of goods
- 5 Late payment or unpaid invoices
- 6 Transactions without proper approval

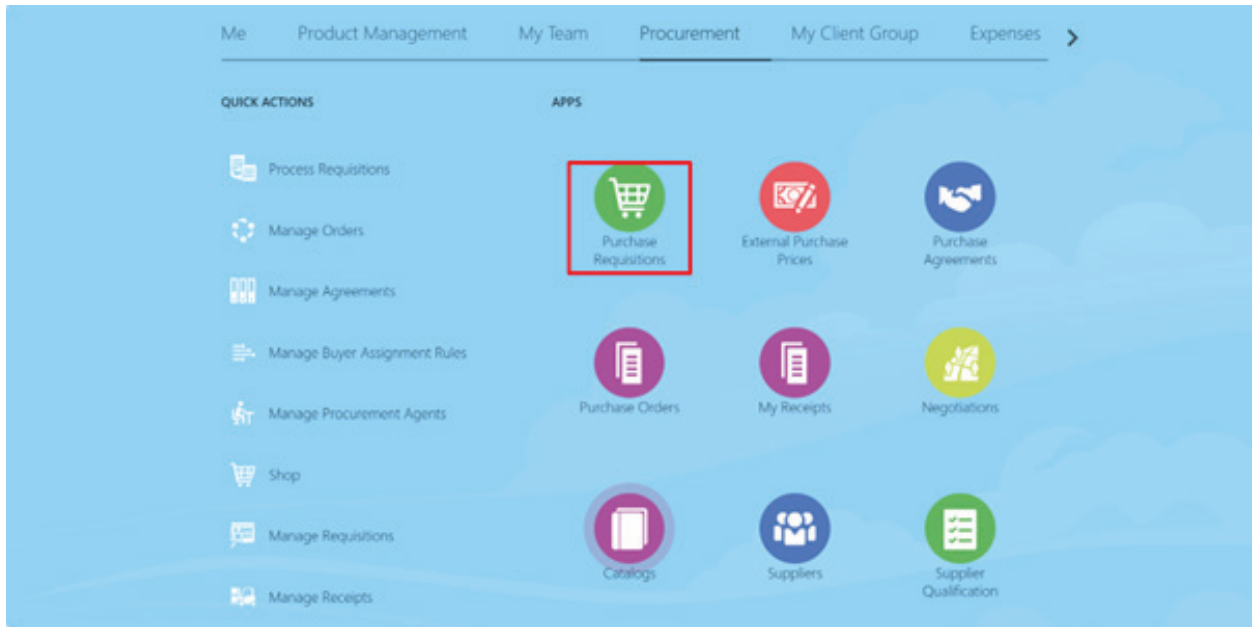
1.2 P2P PROCESS

Having knowledge of the P2P cycle in automated contexts is crucial for auditors. As ERPs eliminate the associated paper work, auditors must conduct the analysis within the system itself.

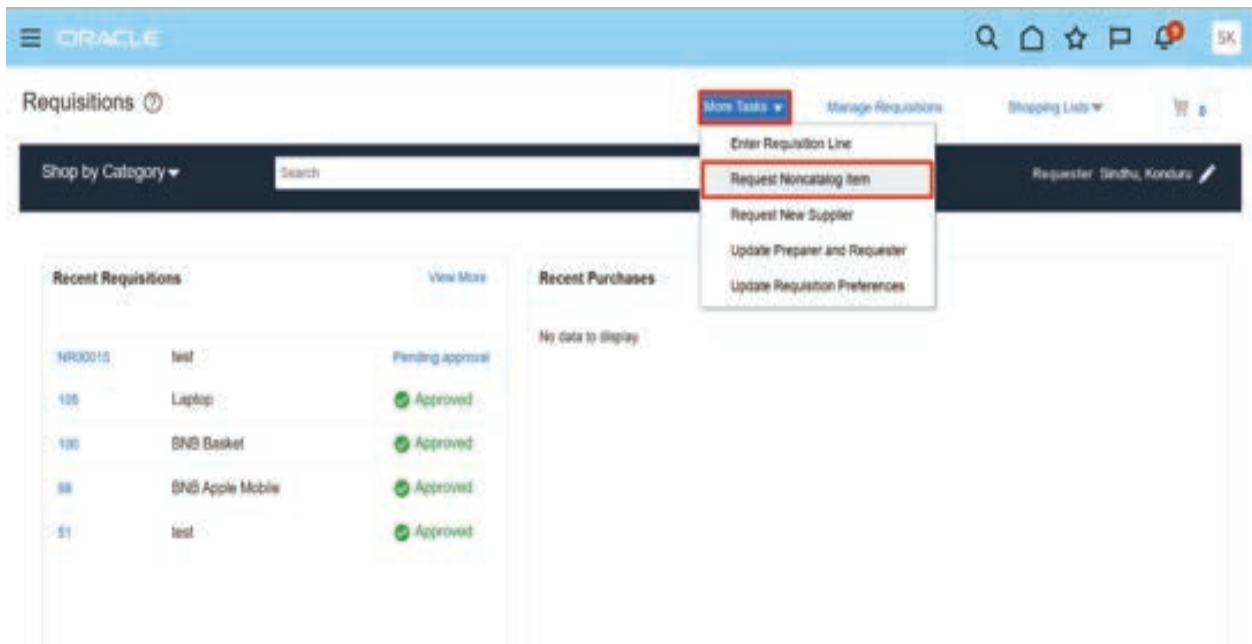
1.2.1 Creating a Purchase Requisition

Creating a Purchase Requisition (PR) is the first step in the Procure-to-Pay Cycle. When an employee has to make a purchase or place an order on behalf of their company, a requisition is the official document used. In Oracle Cloud Fusion, an employee (or a user) creates a PR by navigating to the "Procurements" > "Purchase Requisitions" > "Enter Requisition Line" screen in Oracle Cloud Fusion Work Area.

- i Navigate to: Procurement > Purchase requisition



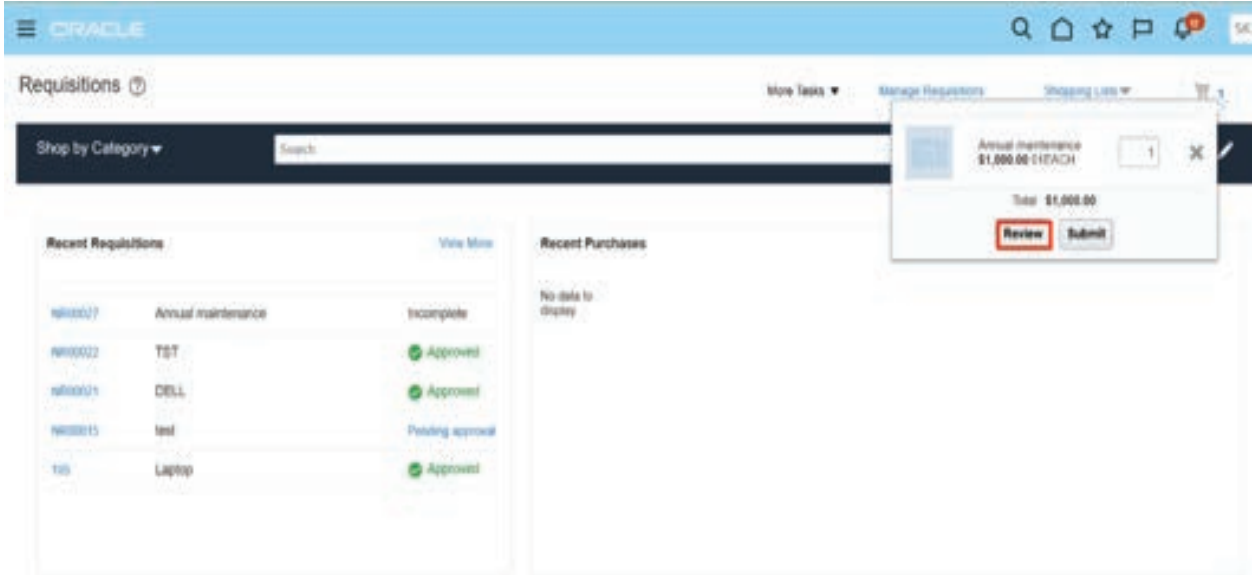
ii Click the more Tasks Dropdown and Select Request Noncatalog Item



iii Enter the Below Requisition Details and click on add to Cart Button.

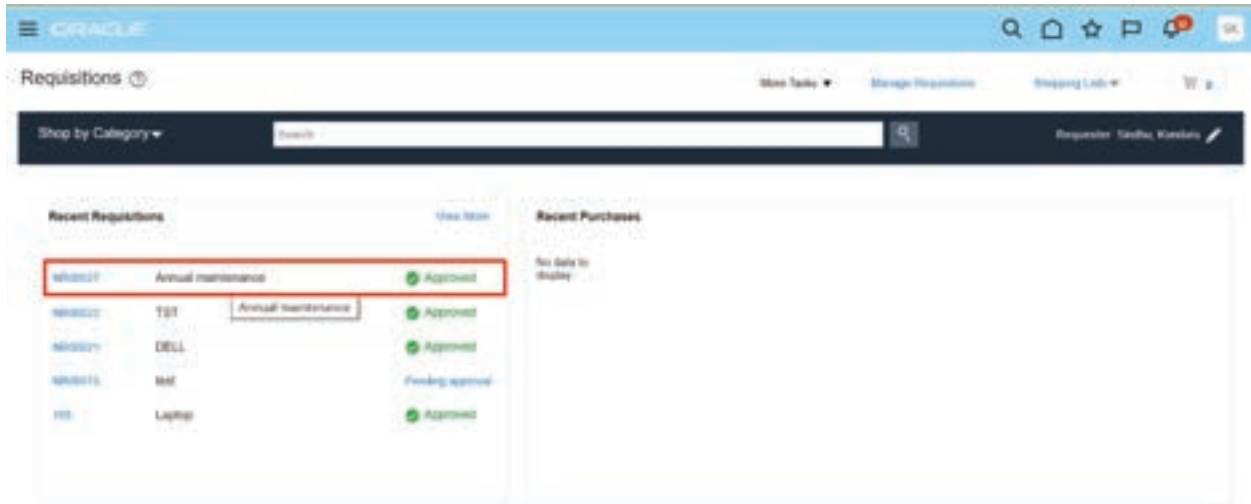
iv Click the more Tasks Dropdown and Select Request Noncatalog Item

- v Click on the Cart and click on the Review Button



- vi Review the requisition details and click on submit button.

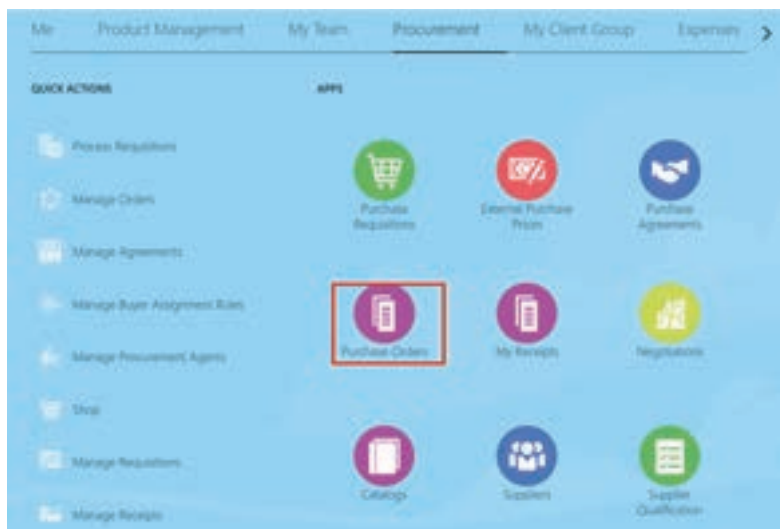




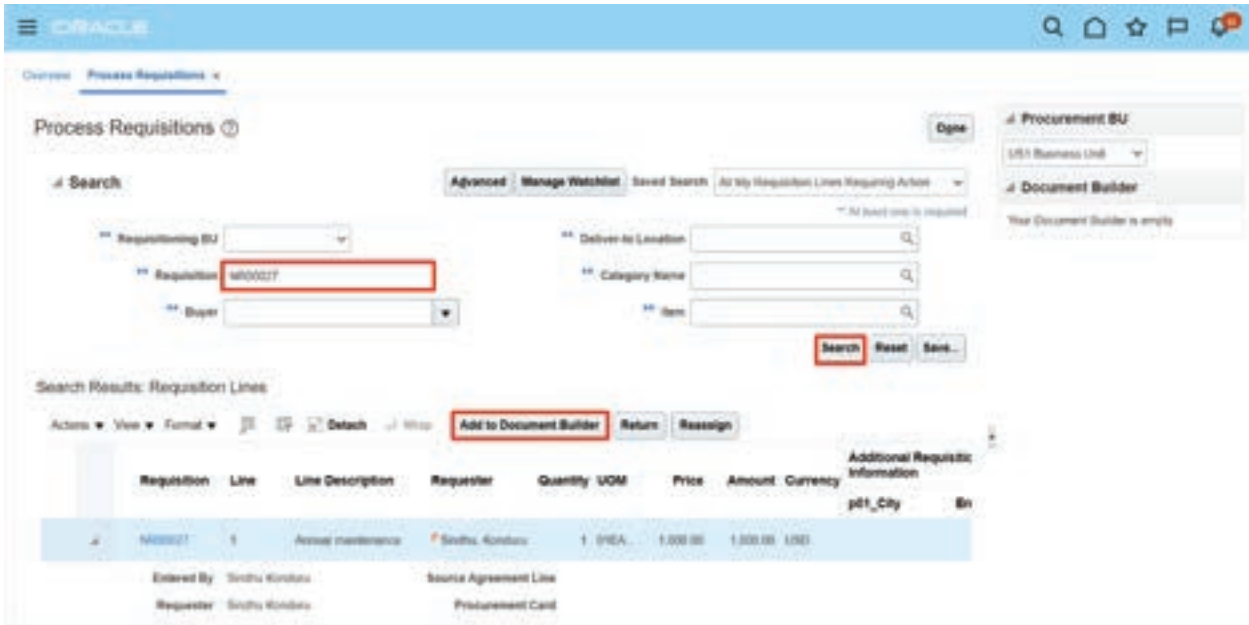
1.2.2 Create Purchase Order with Requisition.

A Purchase Order (PO), a legal document defining the terms of the sale, may be created by you when a quotation is accepted by Purchasing.

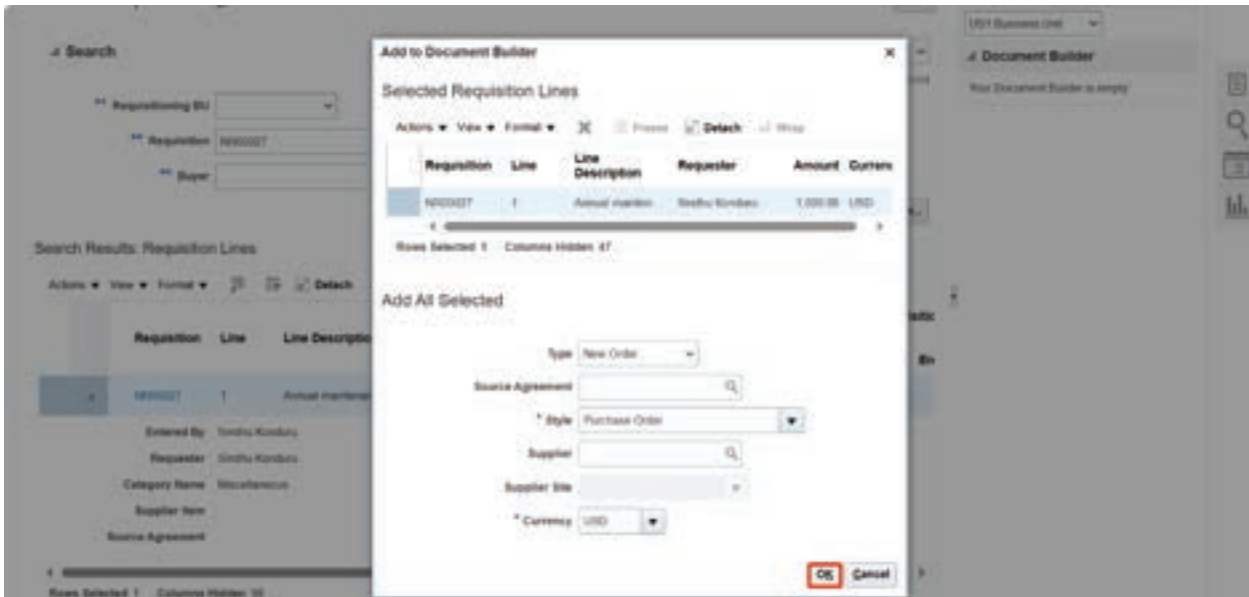
The PO document specifies the purchase's terms and conditions, as well as the cost, quantity, and need-by date of the requested products or services. The Supplier Item Catalogue form can be utilised to retrieve quotation information when creating a PO (manually or automatically from requisitions). Additionally, the PO contains information like the Ship To address, supplier details, distribution accounts, and purchasing criteria. The PO is broken down into portions called PO header and PO lines.



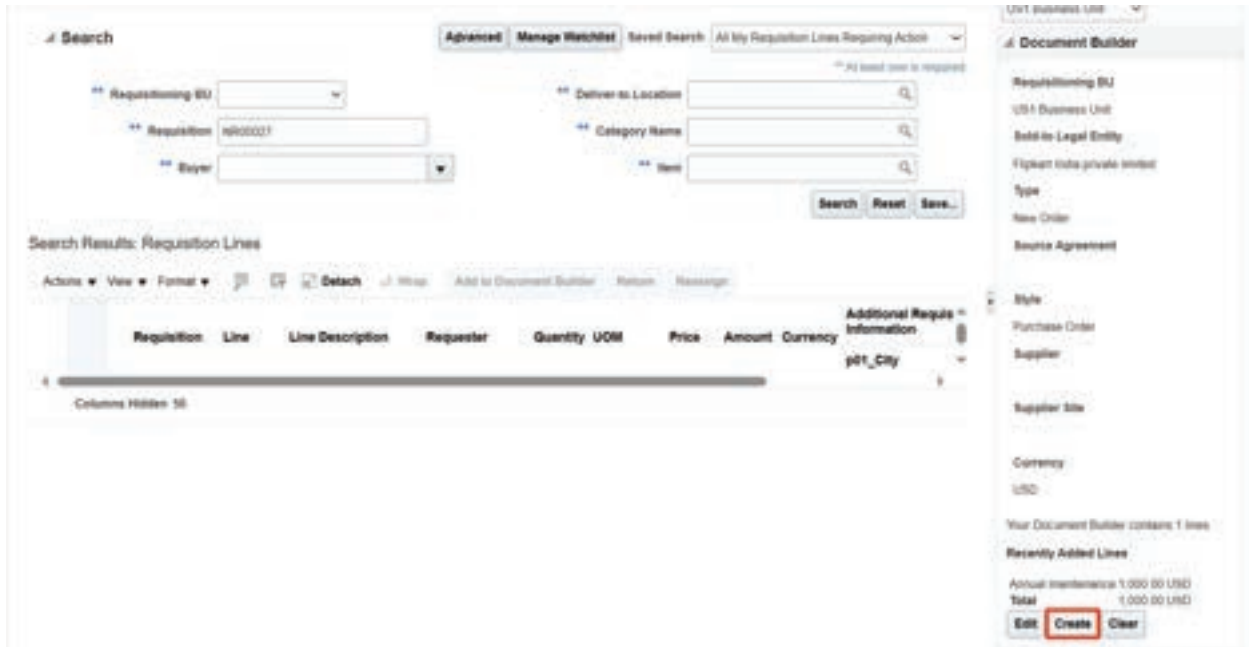
- i Click on the tasks and click on the **process requisition** task from Requisition.
- ii Search with requisition and select the requisition and click on **Add on Document Builders** Button.



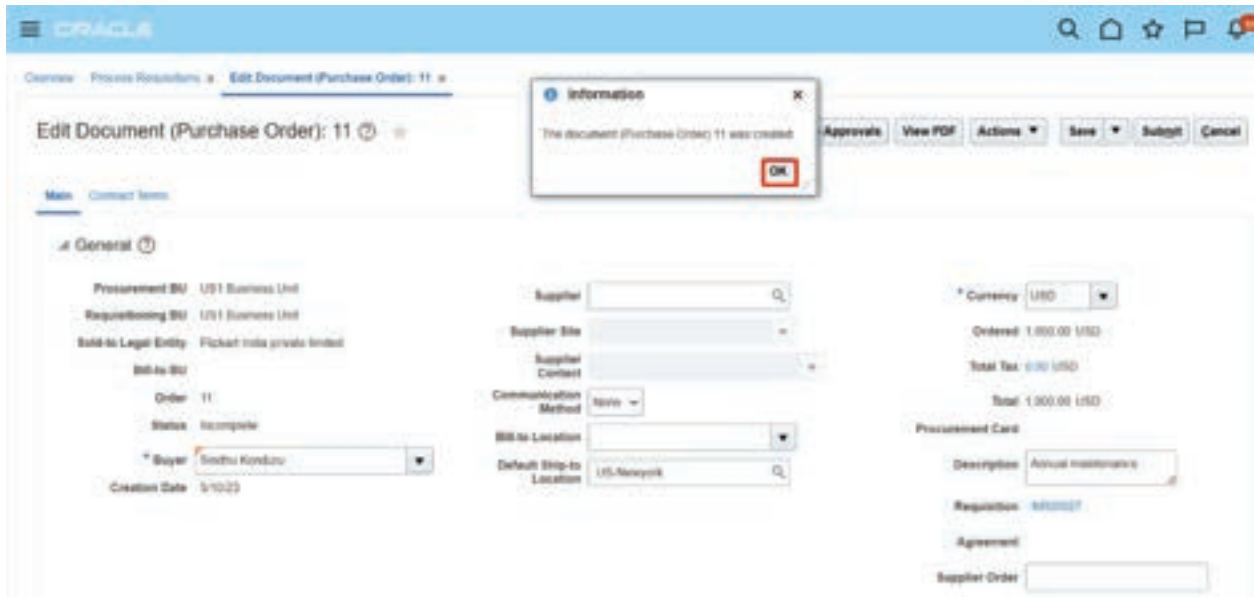
- iii Select on the line and click on Ok button



iv Click on the create button to create order.



v It will create the order and generate the order number



vi Verify the details and click on submit button.

Oracle Procurement Edit Document (Purchase Order): 11

Buttons: Manage Approvals, View PDF, Actions, Save, **Submit**, Cancel

Main Contract Terms

General

Procurement BU: US1 Business Unit
 Requisitioning BU: US1 Business Unit
 Sold-to Legal Entity: Flipkart India (private limited)
 Bill-to BU: US1 Business Unit
 Order #: 11
 Status: Incomplete
 * Buyer: Sridhar Kombaru
 Creation Date: 5/19/23

Supplier: [Search]
 Supplier Site: [Dropdown]
 Supplier Contact: [Dropdown]
 Communication Method: None
 Bill-to Location: [Dropdown]
 Default Ship-to Location: US-Newyork

* Currency: USD
 Ordered: 1,000.00 USD
 Total Tax: 0.00 USD
 Total: 1,000.00 USD

Procurement Card
 Description: Annual maintenance
 Requisition: NR0001
 Agreement
 Supplier Order: [Text Box]

Terms, Notes and Attachments

Oracle Procurement Edit Document (Purchase Order): 11

Buttons: Manage Approvals, View PDF, Actions, Save, **Submit**, Cancel

Main Contract Terms

General

Procurement BU: US1 Business Unit
 Requisitioning BU: US1 Business Unit
 Sold-to Legal Entity: Flipkart India (private limited)
 Bill-to BU: US1 Business Unit
 Order #: 11
 Status: Incomplete
 * Buyer: Sridhar Kombaru
 Creation Date: 5/19/23

Supplier: **MURALI TECHNOLOGIES**
 Supplier Site: United states
 Supplier Contact: tech, murali
 Communication Method: None
 Bill-to Location: New York Ad
 Default Ship-to Location: US-Newyork

* Currency: USD
 Ordered: 1,000.00 USD
 Total Tax: 0.00 USD
 Total: 1,000.00 USD

Procurement Card
 Description: Annual maintenance
 Requisition: NR0007
 Agreement
 Supplier Order: [Text Box]

vii It will submit for manager approval.

Confirmation

The document (Purchase Order) 11 was submitted for approval

View PDF Actions Refresh Done

Purchase Order: 11

Main

General

Procurement BU: US1 Business Unit
 Requisitioning BU: US1 Business Unit
 Sold-to Legal Entity: Flipkart India private limited
 Bill-to BU: US1 Business Unit
 Order: 11
 Status: **Incomplete**
 Buyer: Anitha, Konda
 Creation Date: 5/10/23

Supplier: MURALI TECHNOLOGIES
 Supplier Site: United States
 Supplier Contact: Prasad tech
 Communication Method: None
 Bill-to Location: New York A,
 Ship-to Location: US-Newyork

Ordered: 1,000.00 USD
 Total Tax: 0.00 USD
 Total: 1,000.00 USD
 Description: Annual maintenance
 Requisition: NPO0001
 Source Agreement
 Supplier Order
 Master Contract

Terms **Notes and Attachments**

Payment Terms: 30 Net 2%, 60 Net 1%
 Shipping Method:
 Freight Terms:
 Requires signature
 Buyer Managed Transportation

Confirmation

The document (Purchase Order) 11 was submitted for approval

View PDF Actions Refresh Done

Purchase Order: 11

Main

General

Procurement BU: US1 Business Unit
 Requisitioning BU: US1 Business Unit
 Sold-to Legal Entity: Flipkart India private limited
 Bill-to BU: US1 Business Unit
 Order: 11
 Status: **Open**
 Buyer: Anitha, Konda
 Creation Date: 5/10/23

Supplier: MURALI TECHNOLOGIES
 Supplier Site: United States
 Supplier Contact: Prasad tech
 Communication Method: None
 Bill-to Location: New York A,
 Ship-to Location: US-Newyork

Ordered: 1,000.00 USD
 Total Tax: 0.00 USD
 Total: 1,000.00 USD
 Description: Annual maintenance
 Requisition: NPO0001
 Source Agreement
 Supplier Order
 Master Contract

Order Life Cycle

Ordered

0.0 0.4K 0.8K 1.2K

Amount (USD)

View Details

Terms **Notes and Attachments**

Payment Terms: 30 Net 2%, 60 Net 1%
 Shipping Method:
 Freight Terms:
 Requires signature
 Buyer Managed Transportation

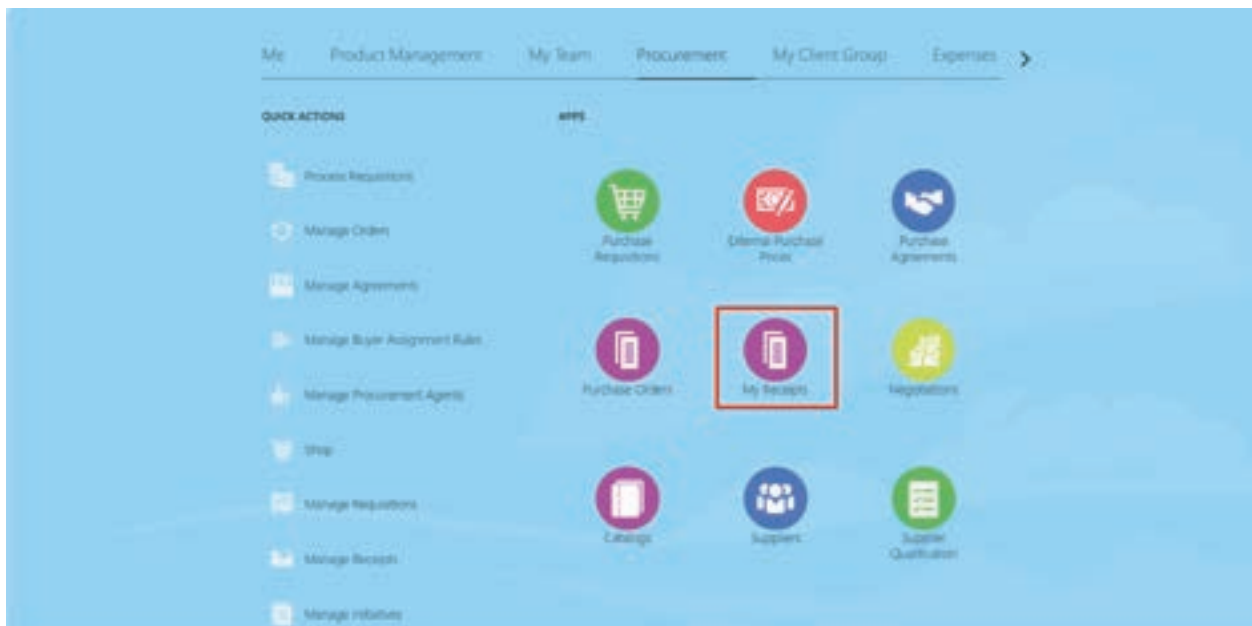
1.2.3 Receive Goods

Once the vendor has placed the order and dispatched the goods/services, they must travel to the intended location. Entering the quantity (approved quantity) and/or receiving location into Oracle Purchasing's receiving form completes the receipt.

creating receipts and records for commodities arriving at the distribution centre and entering them into the warehouse system. When a supplier provides goods or services, the necessary receiving information is entered, and line items are checked to make sure that everything ordered has been delivered.

The receiving form will have fields for the supplier, such as the ship-to address and the delivery date. Once all of the data has been entered, this is finished.

Navigation: procurement > My Receipt



- i Search with requisition or purchase order number and select the line and click on **Receive** Button.

Receive Items

Advanced Search

Requester: []
 Entered By: []
 Requisition: N100027
 Item Due: Any time
 Requisitioning BU: US1 Business Unit
Purchase Order: 11

Purchase Order Line: []
 Transfer Order: []
 Supplier: []
 Shipment: []

Search Reset Save... Add Fields Reorder

Search Results

View: Formatted | Print | Refresh | Detach | Wrap | **Receive**

Requisitioning BU	Requisition	Line	Item Description	Supplier	Need-by Date	Ordered Quantity	UOM Name	Currency	Purchase Order	Transfer Order
US1 Business Unit	N100027	1	Annual maintenance	MURALI TECH.	12-19-23	1	EACH		11	

Rows Selected: 1 Columns Hidden: 0

ii Enter the receive quantity and click on submit button.

Create Receipts

Submit Cancel

Actions: View Formatted | Print | Refresh | Detach | Wrap | Refresh Line | Show Receipt Quantity

Requisition	Item Description	Receipt Quantity	UOM Name	Currency	Transaction Date	Waybill	Packing Slip	Requisitioning BU	Purchase Order	Transfer Order
N100027	Annual maintenance	1	EACH		5/10/23 8:27			US1 Business Unit	11	

Rows Selected: 1 Columns Hidden: 0

iii Receipt number will be generated.

Create Receipts

Submit Cancel

Actions: View Formatted | Print | Refresh | Detach | Wrap | Refresh Line | Show Receipt Quantity

Requisition	Item Description	Receipt Quantity	UOM Name	Currency	Transaction Date	Waybill	Packing Slip	Requisitioning BU	Purchase Order	Transfer Order
N100027	Annual maintenance	1	EACH		5/10/23 8:27			US1 Business Unit	11	

Rows Selected: 1 Columns Hidden: 0

Confirmation

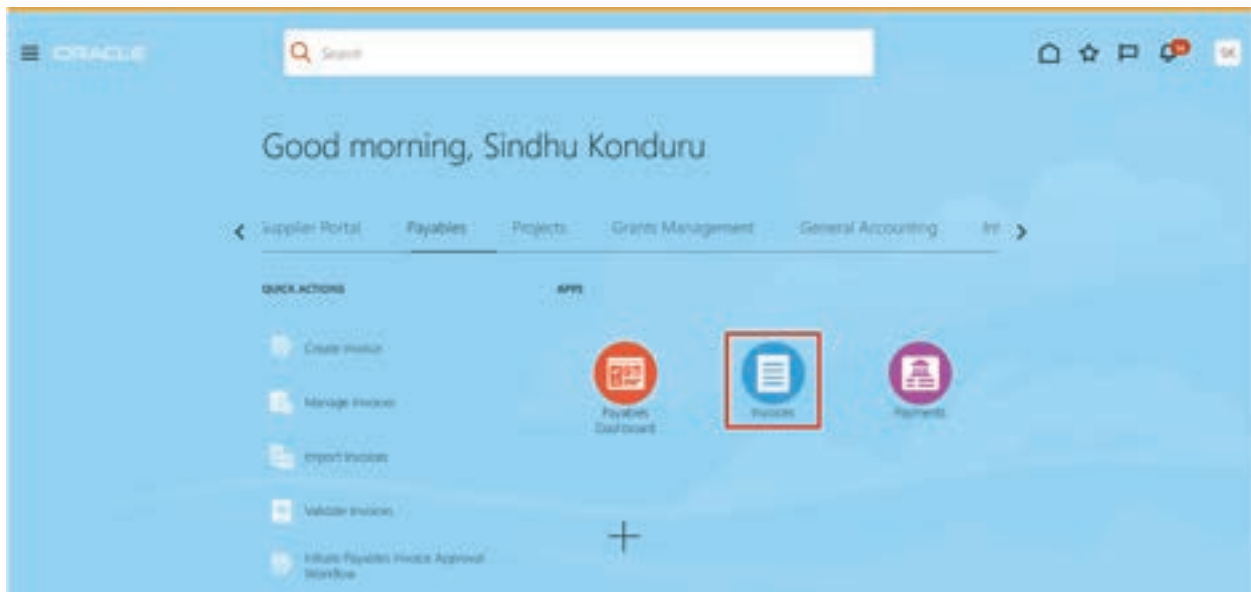
You created the following receipt numbers: 102

OK

1.2.4 Create payable invoice with matched PO number

Once the receipt is entered, the invoice can be created in Oracle. An invoice specifies the price of the goods or services and any other terms, and an essential aspect of the invoice includes a due date for payment.

Navigation: Payable > Invoices



- i Click on the create invoice link from invoices task



- ii Search with po number and enter the invoice details and select the **match invoice line** and click on the **GO** button.

- iii Select the po and click on Apply, Ok button.

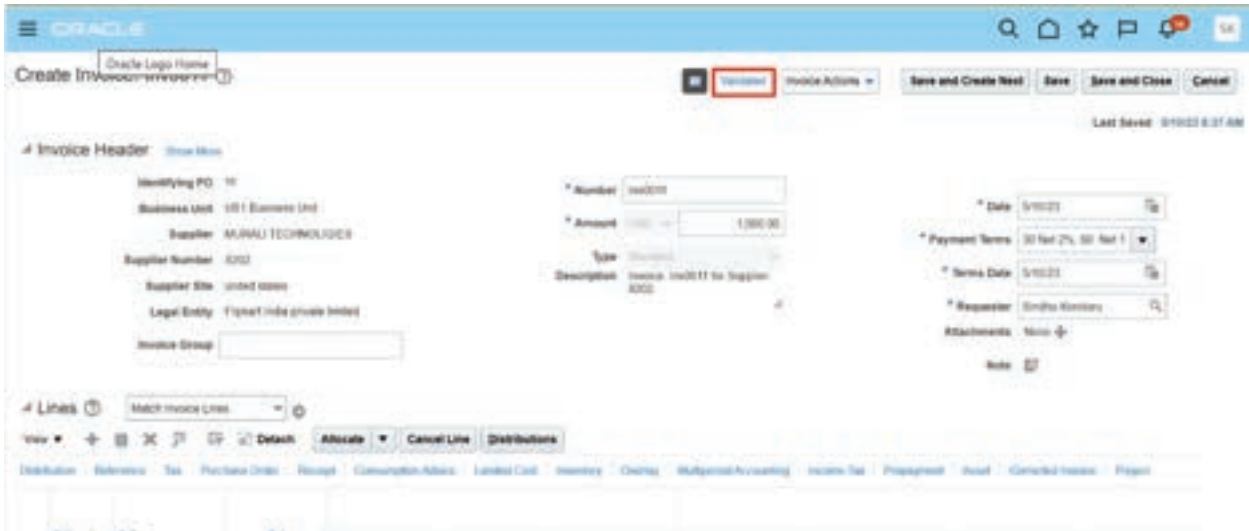
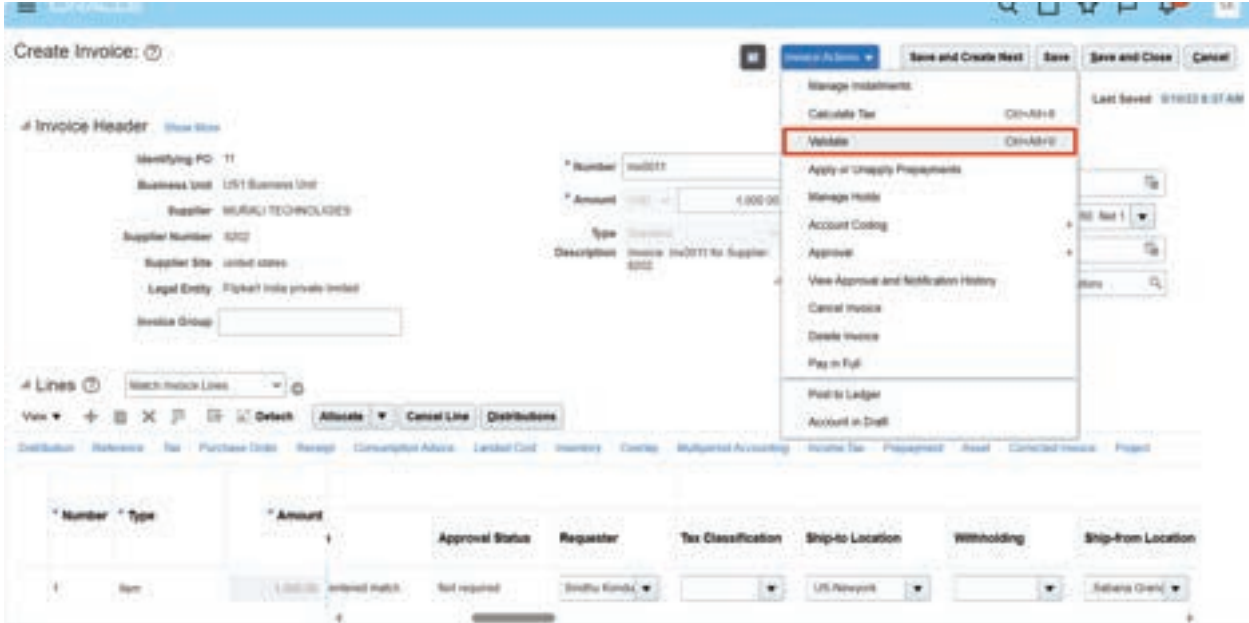
Match	Line	Quantity	Unit Price	Amount	Item Description	Purchase Order Number	Line	Schedule Number	Receipt Number	Line	Ship-to Location	Need-by Date	Item Number
<input checked="" type="checkbox"/>	1	1	1,000.00	1,000.00	Account maintenance	11	1	1	102	1	115-Newyork	12/10/23	
				Total									
					1,000.00								

PO 11, Line 1, Schedule 1: Details

Ordered	1	Received	1	WOM	STLAC1
Available	1	Accepted	0	Match Basis	Quantity
Billed	0	Returned	0	Invoice Match Option	Receipt
Shipped	0	Consumed	N/A	Payment Terms	30 Net 2%, 90 Net 1%
				Freight Terms	

Buttons: Apply, OK, Cancel

- v Validate the invoice, click on invoice actions > validate.



1.2.5 Manage Invoices

To search the invoices

- i Navigate to Payables > Invoices > Manage Invoices

The screenshot shows the Oracle Invoices dashboard. At the top, there are navigation icons for 'Payables', 'Invoices', and 'Expenses'. Below this, there are four summary cards: 'Recent' (2), 'Hold' (279 Validation, 43 Purchasing, 47 Other), 'Approval' (0 Pending, 0 Other, 49 Rejected), and 'Prepaid' (1, 6, 163). A table below these cards lists invoices with columns: Invoice Number, Amount, Supplier, Supplier Site, Validation Status, Accounting Status, Paid Status, and Creation Date. A sidebar on the right contains a 'Manage Invoices' link highlighted in a red box, along with other options like 'Create Invoice', 'Apply Billing', and 'Accounting'.

- ii Enter the invoice number and click on search

The screenshot shows the 'Manage Invoices' search interface. It features a search bar with the text 'Search: Invoice'. Below the search bar are several input fields: 'Business Unit', 'Invoice Number' (highlighted with a red box and containing '61021'), 'Invoice Amount', 'Invoice Date', and 'Supplier or Party'. To the right, there are fields for 'Supplier Number', 'Supplier Site', 'Company ID', and 'Invoice Group'. A 'Search' button is highlighted with a red box. At the bottom, there is a table with columns: Invoice Number, Invoice Date, Co-Supplier or Co-Party, Supplier Site, Inptd Amount, Invoice Amount, Applied Payments, Invoice Type, Notes, Validation Status, Approval Status, and Hold.

1.2.6 Invoice Payment to Supplier

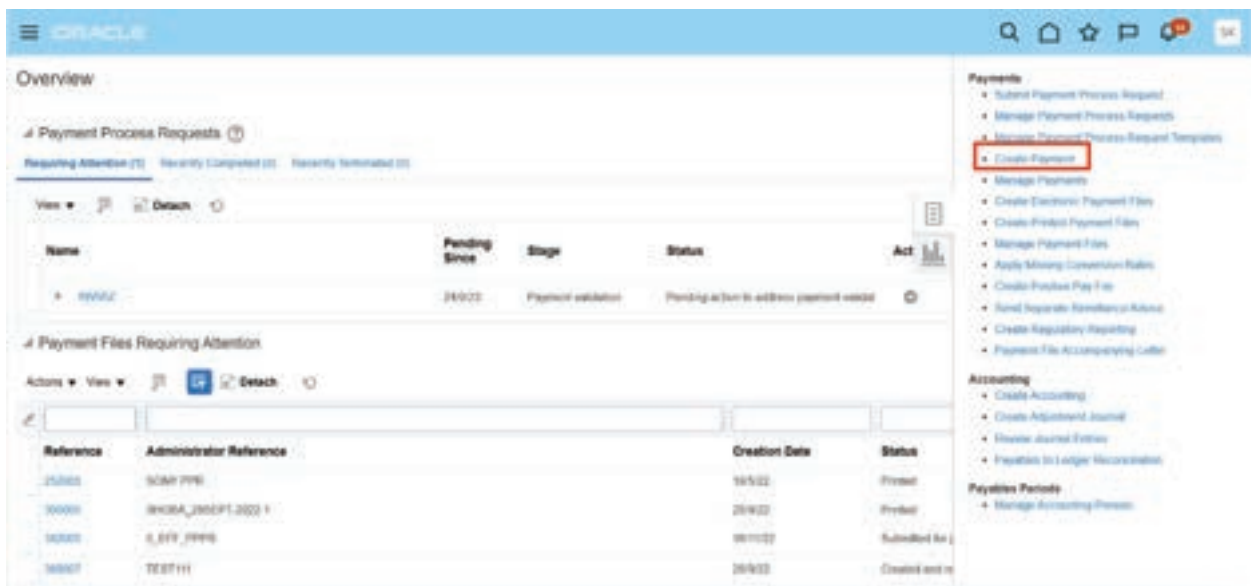
The last step in the P2P cycle in Oracle Cloud Fusion is making the payment to the supplier/vendor. The payment is made by entering the invoice and PO numbers (and/or receipt) into Oracle’s payment form.

The payment form also includes more information about the supplier, ship-to address, and delivery date. After these are entered, the payment is made and the cycle ends.

- i Navigation: Payables > Payments.



- ii Click on the create payment Button.



iii Enter the mandatory Information's.

Create Payment

Payment Details | Advanced | Additional Information

* Business Unit: US1 Business Unit

* Supplier of Party: MURALI TECHNOLOGIES

* Supplier Site: united states
Address: Subana Grande, Puerto Rico 00907 United States, Subana Grande

* Payment Date: 5/10/23

* Type: Check

Description:

* Disbursement Bank Account: 0002_0002_AC

* Payment Currency: USD - US Data

* Payment Method: 10 CHECK

* Payment Process Profile: 001_HQI_PER US PAYMENT SYSTEM

Remit to Account: XXXX54116

Remit to Bank Name: Bank of America US

Remit to Branch Name: Newark

Payment Document:

Paper Document Number:

Attachments: None

Invoices to Pay

View | Add Check/Confirm/Over-Pay | Detach

Number	Invoice	Type	Due Date	Unpaid	Discount	Amount	Interest	Tax
No invoices selected								

iv Search the invoice for payment with the invoice number and click on search, then apply.

Create Payment

Select and Add Invoices to Pay

Search

Invoice Number: inv0011

Invoice Amount:

Invoice Type:

Advanced | Saved Search | All Available Invoices

Number Number

Invoices Due Today

Search | Reset | Save

Number	Invoice Business Unit	Due Date	Unpaid Amount	Type	Pay Alone
inv001	US1 Business Unit	3/15/23	100.00 USD	Standard	No
inv0011	US1 Business Unit	5/10/23	1,000.00 USD	Standard	No

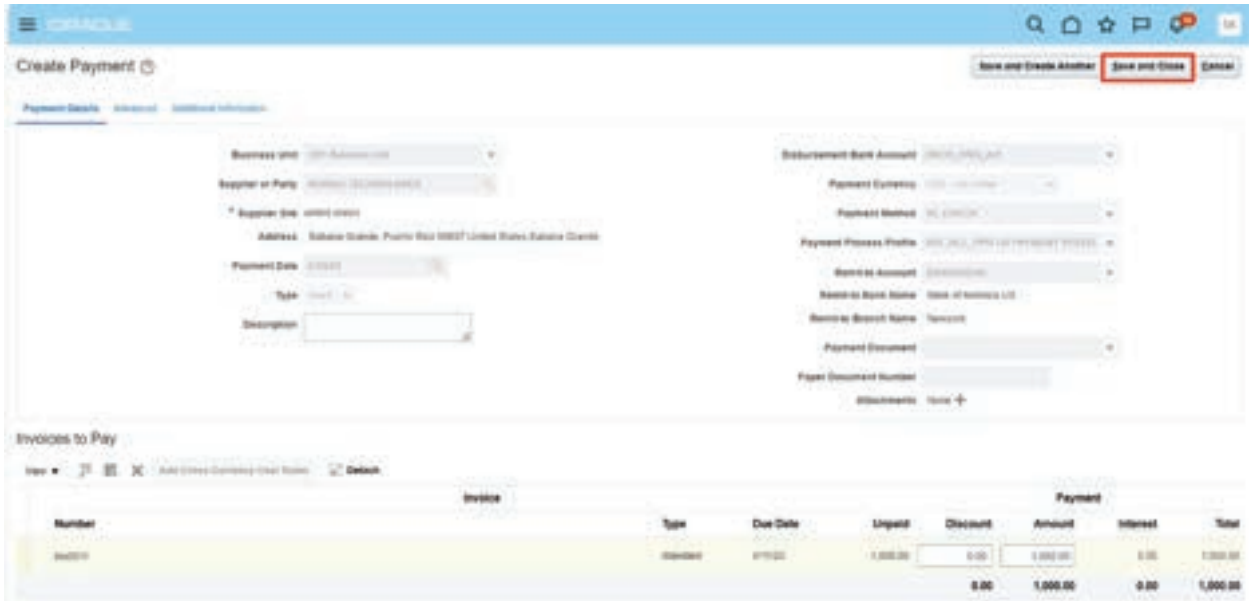
Apply | OK | Cancel

Invoices to Pay

View | Add Check/Confirm/Over-Pay | Detach

Invoice | Payment

- v Then save and close.



- vi The payment has been confirmed.



- vii To view the payment accounting

Navigate to Actions > View Accounting



1.3 MANAGE PAYMENTS

Users can use the payment number to look for a specific payment in the manage payments window or the supplier name to search for payments made to a certain supplier.

i Navigate to Manage Payments



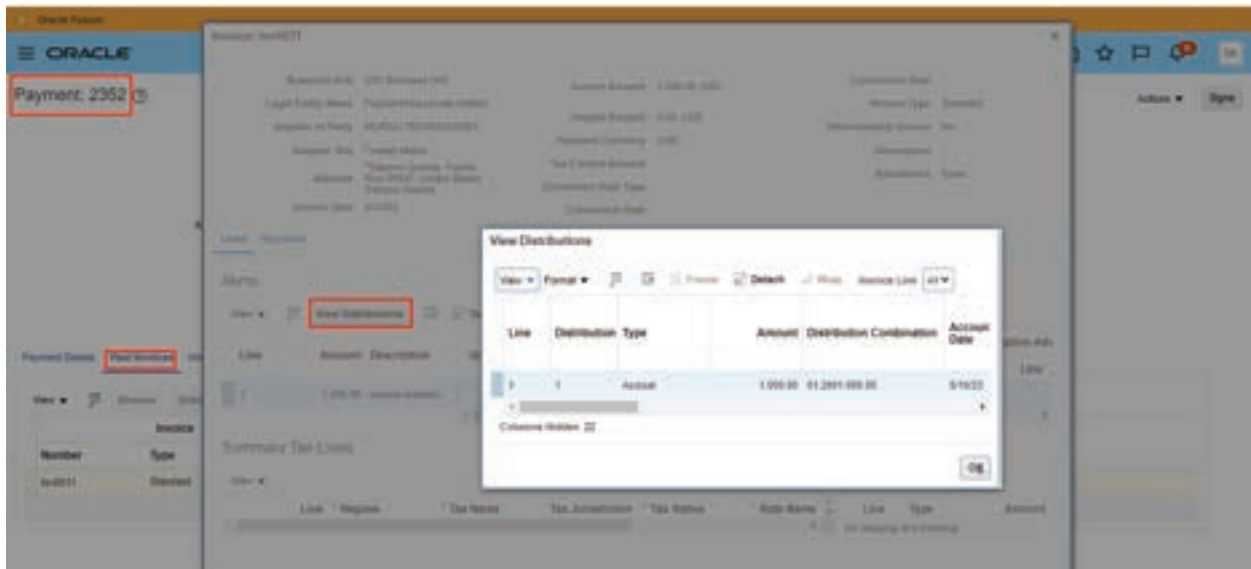
ii Enter the Payment Number and Click on Search



iii Click on the invoice number under the Paid Invoices tab



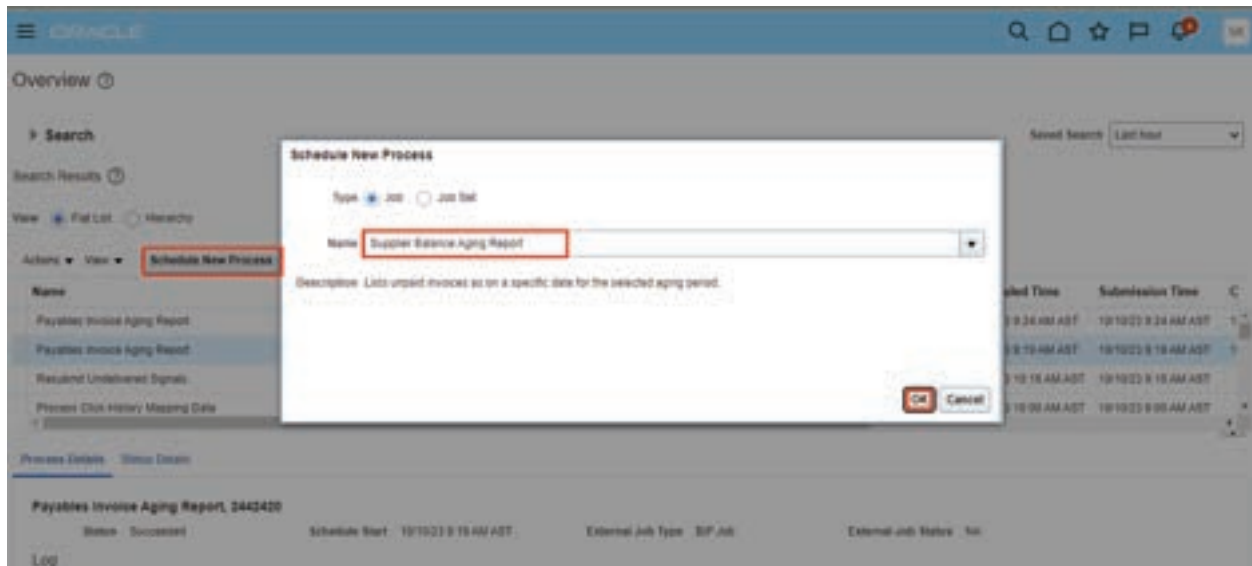
iv User can drilldown to the invoice and distribution from the payment screen.

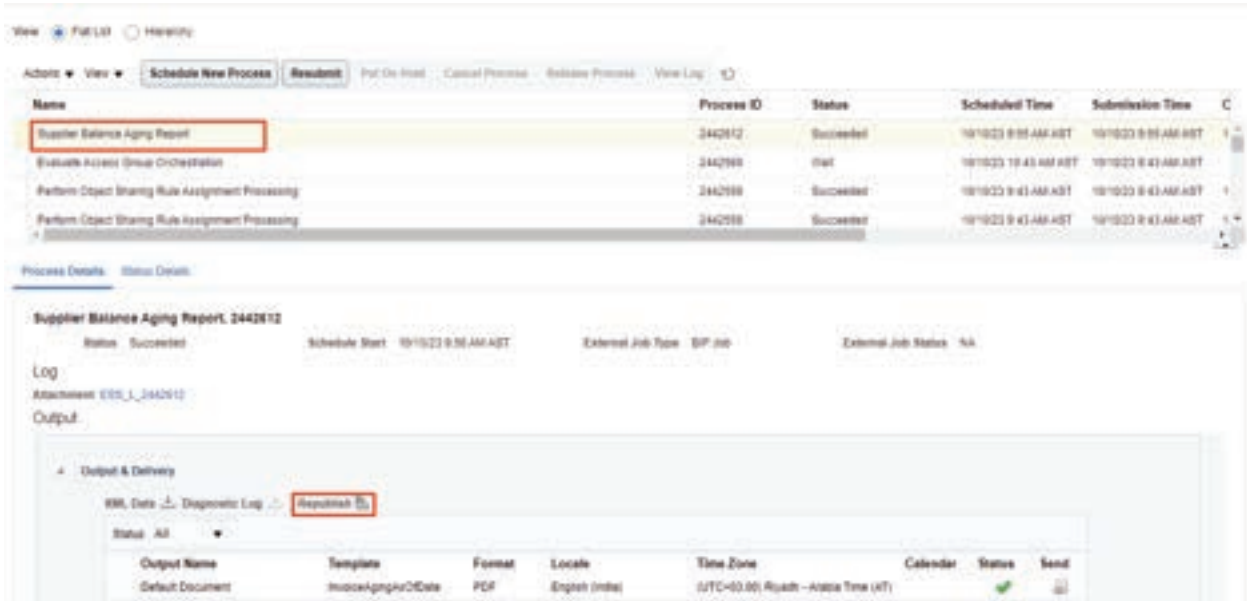


1.4 REPORTS IN P2P CYCLE

1.4.1 Supplier Balance Aging Report

Use the aging report to view the supplier balances according to specified aging periods. The report provides the breakdown of the Payables supplier balance across aging buckets that you configure in the aging periods.





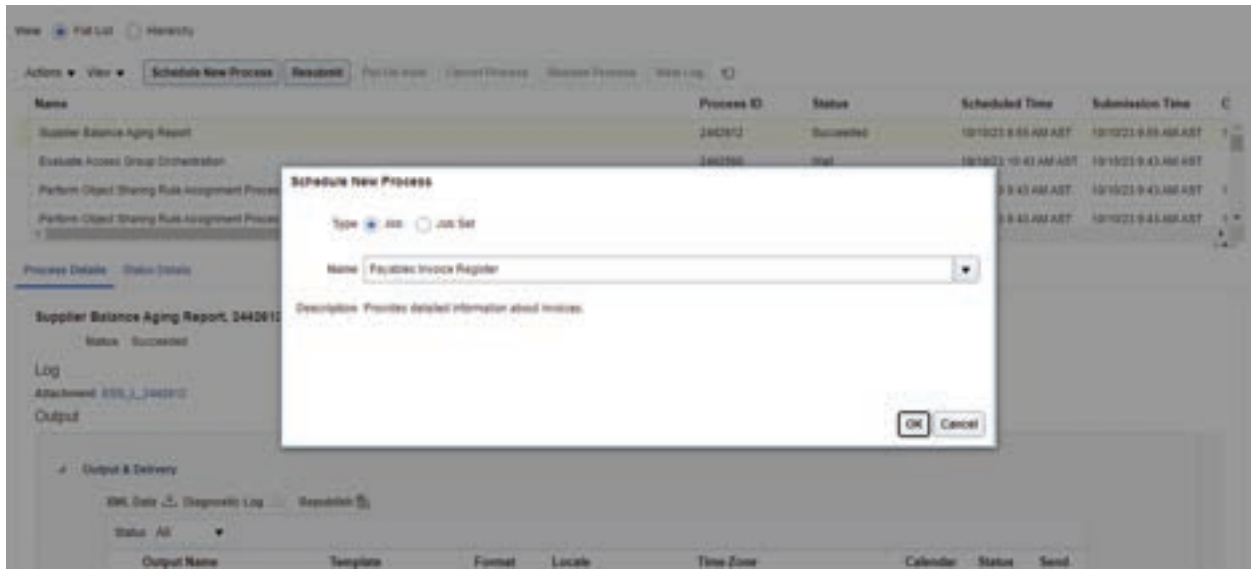
Supplier Balance Aging Report

Supplier Site: Advantage Corp
FLORHAM PARK

Invoice Number	Invoice Amount	Unpaid Amount	Future	1 week Overdue	2 weeks Overdue	3 weeks Overdue	Unallocated Amount
Scrum Flow28-1	1,100.00	1,100.00	0.00	0.00	1,100.00	0.00	0.00
Total for Site FLORHAM PARK	1,100.00	1,100.00	0.00	0.00	1,100.00	0.00	0.00
			0.00%	0.00%	100.00%	0.00%	0.00%
Total for Supplier Advantage Corp	1,100.00	1,100.00	0.00	0.00	1,100.00	0.00	0.00
			0.00%	0.00%	100.00%	0.00%	0.00%
Total for Report	1,100.00	1,100.00	0.00	0.00	1,100.00	0.00	0.00
			0.00%	0.00%	100.00%	0.00%	0.00%

1.4.2 Payables invoice Register

The Payables Invoice Register provides detailed information about invoices. Run the report for a specific invoice group, date range, accounting period. You can also specify an invoice status, such as validated or canceled.



ORACLE		Payables Invoice Register			Report Date: 7/17/14 4:33 AM		
Vision Operations (USA)					Page: 1 of 3		
Currency	USD	Invoice Group	NA	Invoice Type	Standard	Amount Remaining	7,452.25
Supplier Name	Brighton Construction Inc.	Invoice Number	663326	Invoice Date	2/16/14	Original Amount	7,452.25
Description							
Line Number	1	Line Type	Item	Line Amount	7,350.00		
Line Description							
Distribution Number	Distribution Type	Account	Amount	Accounting Date	Income Tax Type	Accounted	
1	Item	01-520-5320-0000-000	4,410.00	2/16/14		Processed	
2	Item	01-500-5320-0000-000	2,940.00	2/16/14		Processed	

CHAPTER 2

ORDER TO CASH AUDIT

2.1 WHY O2C AUDIT IS REQUIRED.

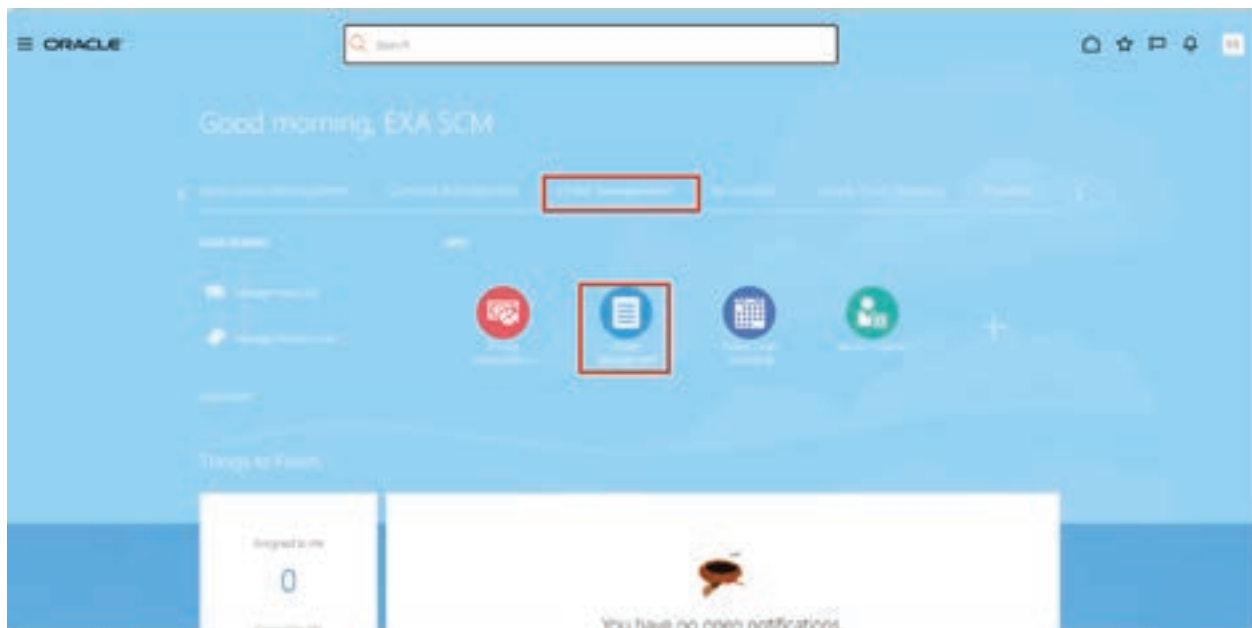
The Order-to-Cash (OTC) process is the set of activities that begin when a customer places an order and ends when payment is received and the order is fulfilled. The OTC process is critical to the success of any organization, as it represents the flow of revenue into the company.

2.2 O2C PROCESS

2.2.1 Create Sales Order

This is the first stage where Order is entered into the system

- i Navigate to Order Management > Order Management

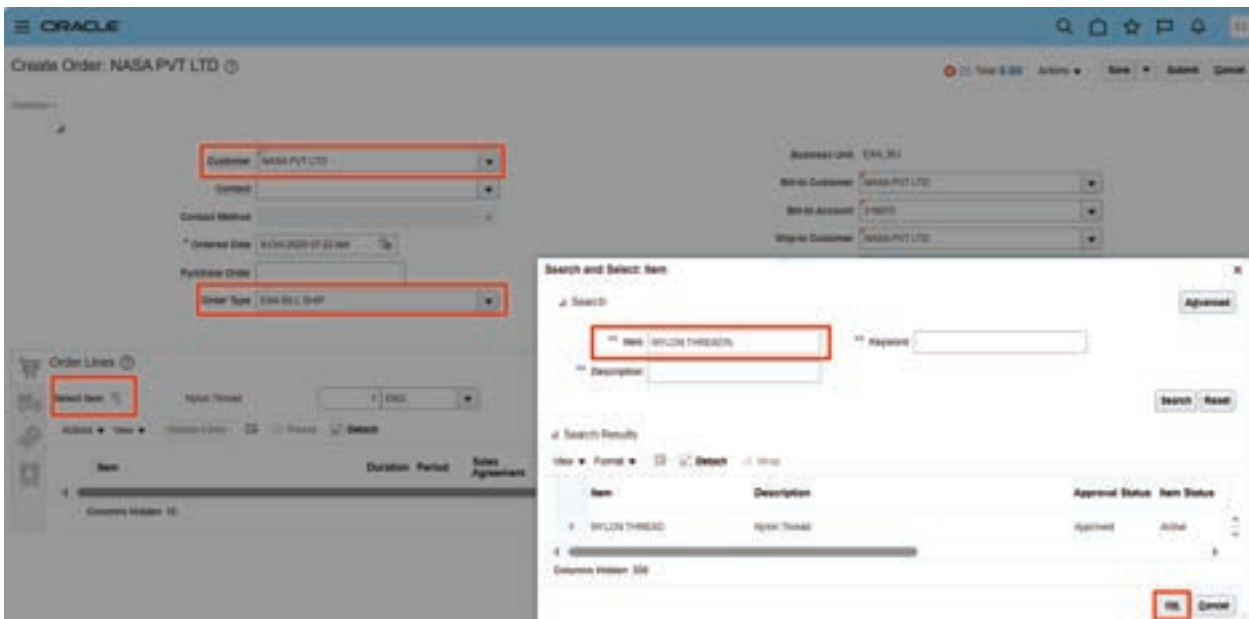


- ii Click on Create Order Button



iii Enter the customer details, Order type and search for the item

iv Select the item and click on Ok



- v Provide the Warehouse details in the Supply Tab

The screenshot shows the Oracle 'Create Order' interface for 'NASA PVT LTD'. The 'Supply' tab is active, and the 'Warehouse' dropdown menu is highlighted with a red box. The dropdown shows 'ORA_PVT000 - Eastern US (0)'. Other fields include Customer (NASA PVT LTD), Order Date (9-02-2023 07:22 AM), and Order Type (ORA-BILL SHIP). The 'Business Unit' is ORA_001, and the 'Ship-to Address' is NASA COLLEGE MANAGEMENT New York, New York.

- vi Under the Billing and Payment Details, Provide the payment terms

- vii Bill to address

The screenshot shows the Oracle 'Create Order' interface for 'NASA PVT LTD' with the 'Billing and Payment Details' tab active. The 'Payment Terms' dropdown menu is highlighted with a red box, showing 'Immediate'. The 'Bill-to Address' is also highlighted with a red box, showing 'NASA COLLEGE MANAGEMENT New York, New York'. Other fields include Customer (NASA PVT LTD), Order Date (9-02-2023 07:22 AM), and Order Type (ORA-BILL SHIP). The 'Business Unit' is ORA_001, and the 'Ship-to Address' is NASA COLLEGE MANAGEMENT New York, New York.

viii Click on Ok and Submit the Sales Order

Oracle CRM 'Create Order' form for NASA PVT LTD. The form includes fields for Customer, Contact, Contact Method, Order Date, Purchase Order, Order Type, Business Unit, Billing Customer, Billing Account, Billing Customer, Billing Address, Sales Credits, and Sales Agreement. A 'Submit' button is highlighted with a red box.

ix Order will be submitted and status will be processing

ixx Click on Refresh button. Order line status will be changed to awaiting shipping

Oracle CRM 'Order: NASA PVT LTD' showing the order status as 'Processing'. The 'Refresh' button is highlighted with a red box. Below is a table showing the order line details.

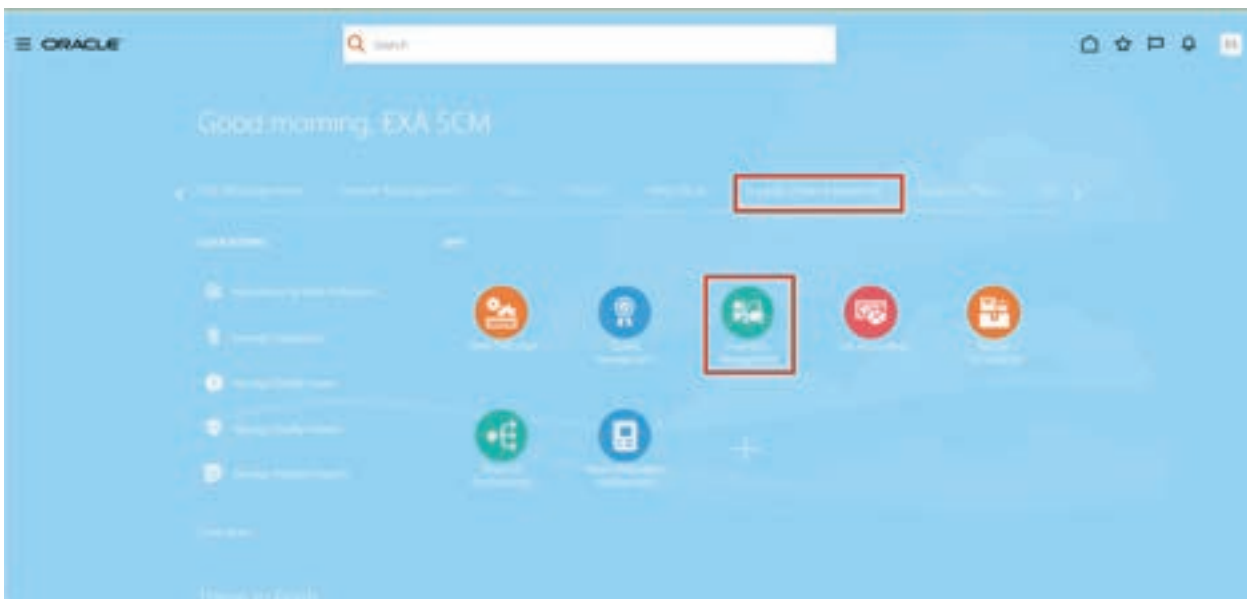
Item	Status	Duration Period	Quantity	Sales Agreement	Sales Agreement Line	Sales Agreement Version	UOM	Secondary Quantity	Secondary UOM	Price	Source UOM
NYC LINE THEBAG - Japan Thread	Awaiting Shipping		1				PCS				



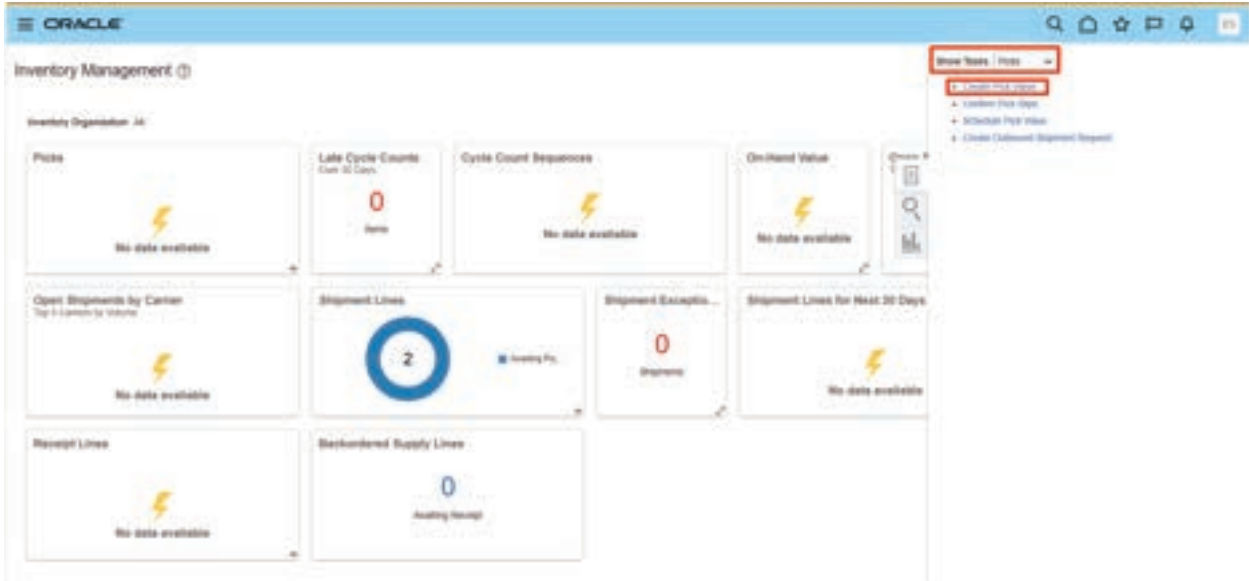
2.2.2 Create Pick Wave

Once the line status is changed to Awaiting Shipping, move the warehouse operations and submit the order for Pick Wave.

- i Navigate to Supply Chain Execution > Inventory Management

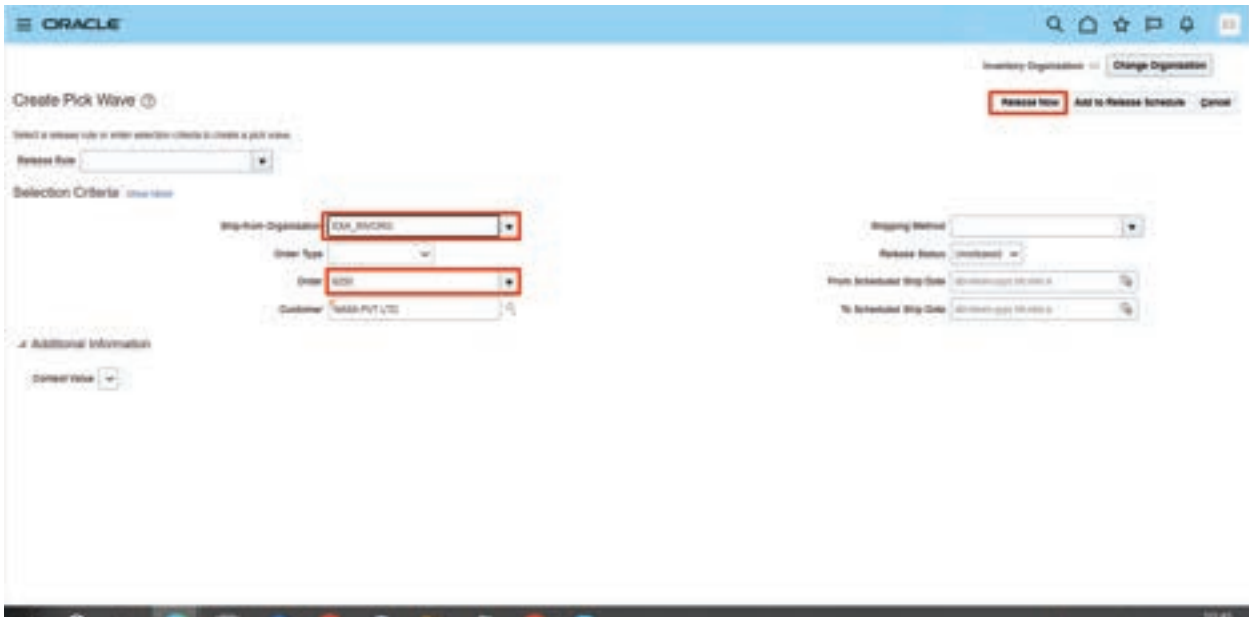


ii Select Picks task and click on Create Pick Wave option



iii Select the Organization name

iv Enter the Order Number and click on Release Now button

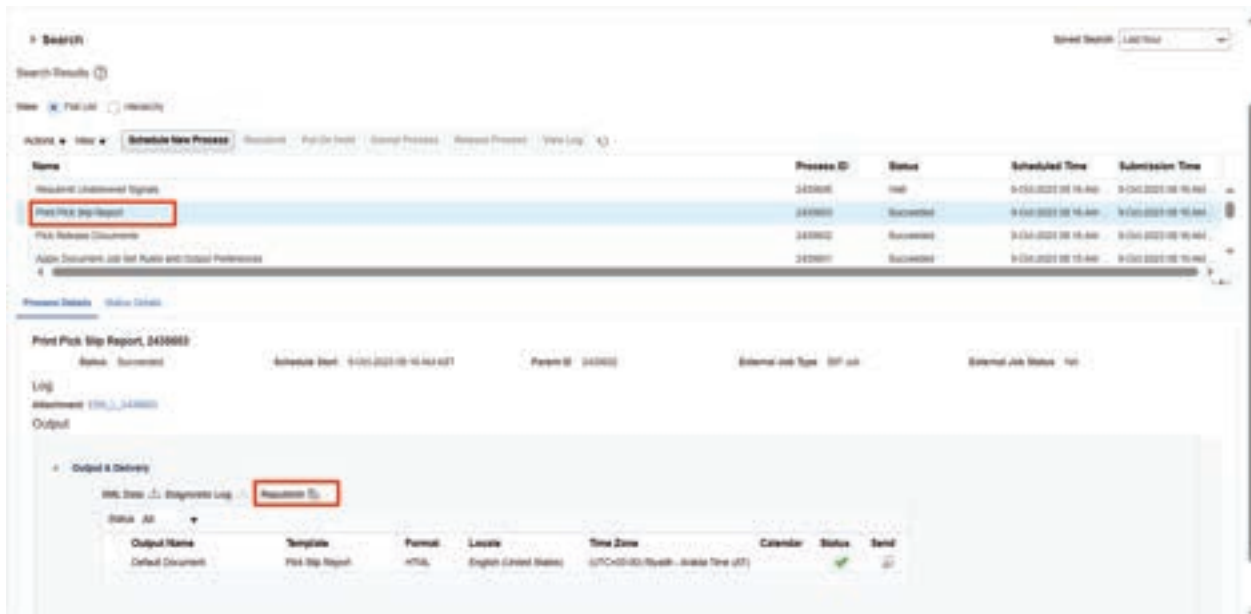


- v Pick Wave number will be generated



- vi Print Pick Slip Report job will be submitted automatically.

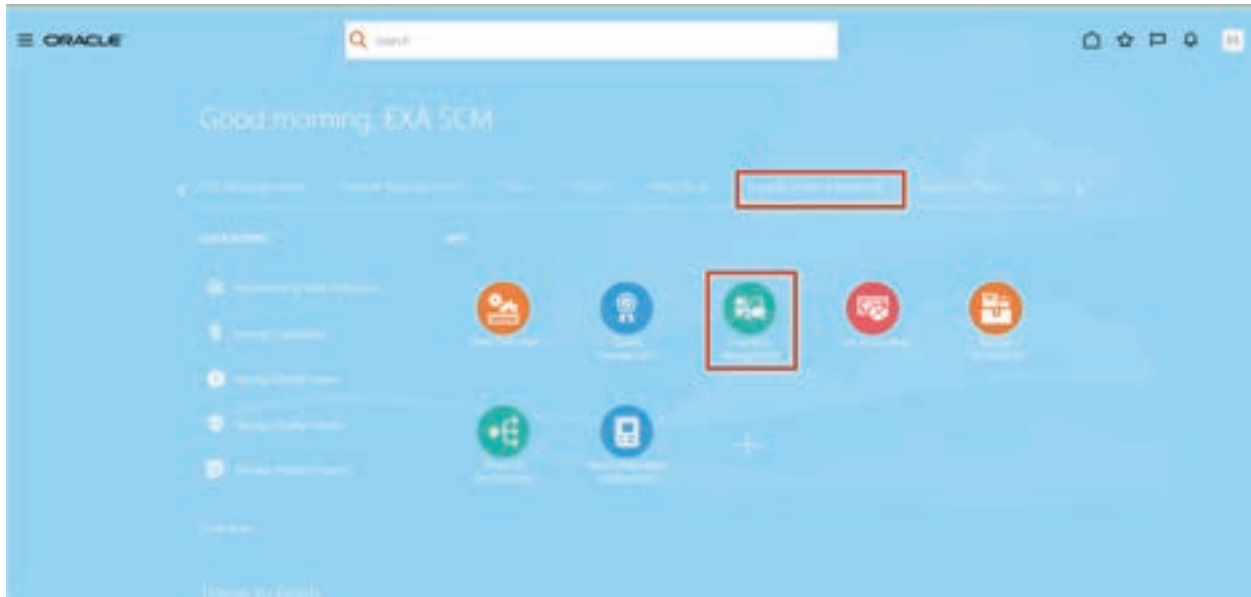
- vii Select the report and click on Republish button to see the report output.



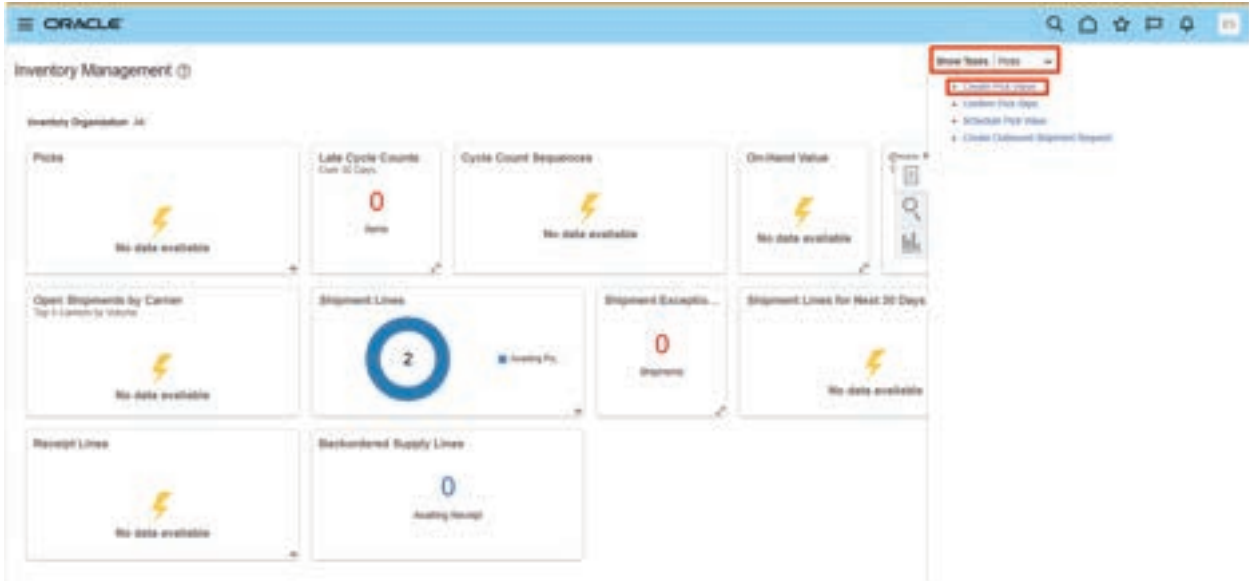
Ship-from Organization		Exacore Inv Org					
Pick Slip	353012	Pick Wave	541084				
Pick Slip Grouping Rule		EXA PICK GRP RULE					
Customer	Shipment	Sales Order #200					
NASA PVT LTD	290018	Shipping Priority					
Ship-to Location		Carrier					
NASA COLONY		Subinventory					
NASAMURK		Requisition					
New York, New York 10001, United States							
Ship-to Contact							
Pick-from Subinventory	Staging Subinventory	Staging Locator					
EXAFRM	EXASTORES						
Movement Request							
541084							
Pick Line	Pick Status	Movement Request Line	Item Revision	Sales Order Pick-from Locator	Sales Order Line Requested Quantity UOM	Shipment Set Requested Quantity	Shipment Shipped Quantity
1	Open	1	NYLON THREAD Nylon Thread	6200 ROW 1 RACK B	1	1	290018
Shipping Instructions							

2.2.3 Create Pick Confirm

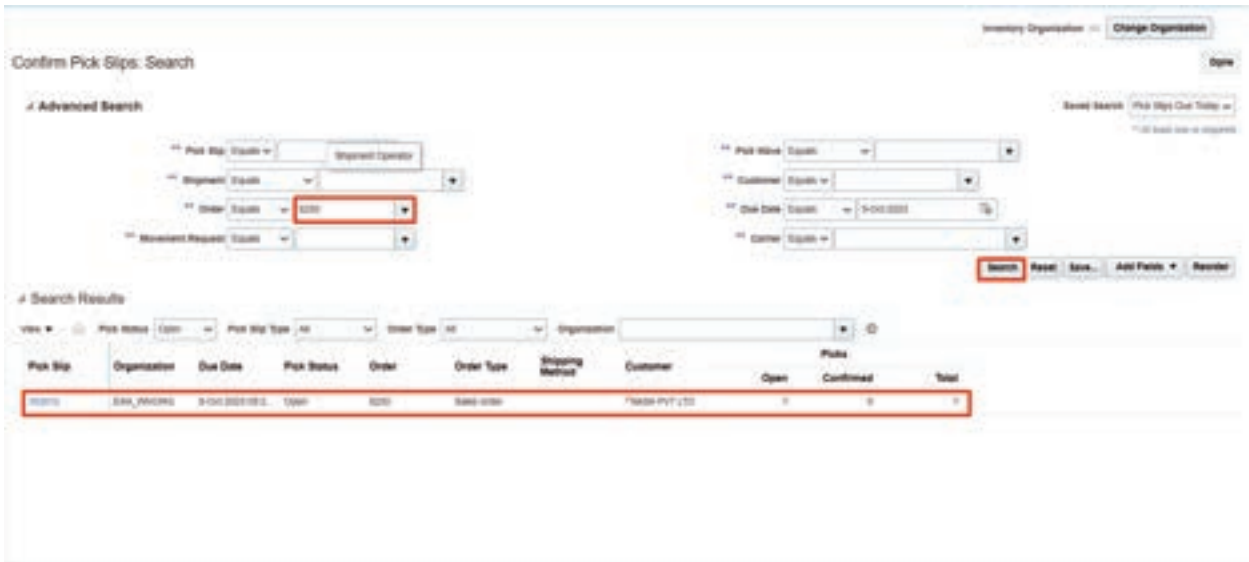
- i Navigate to Supply Chain Execution > Inventory Management



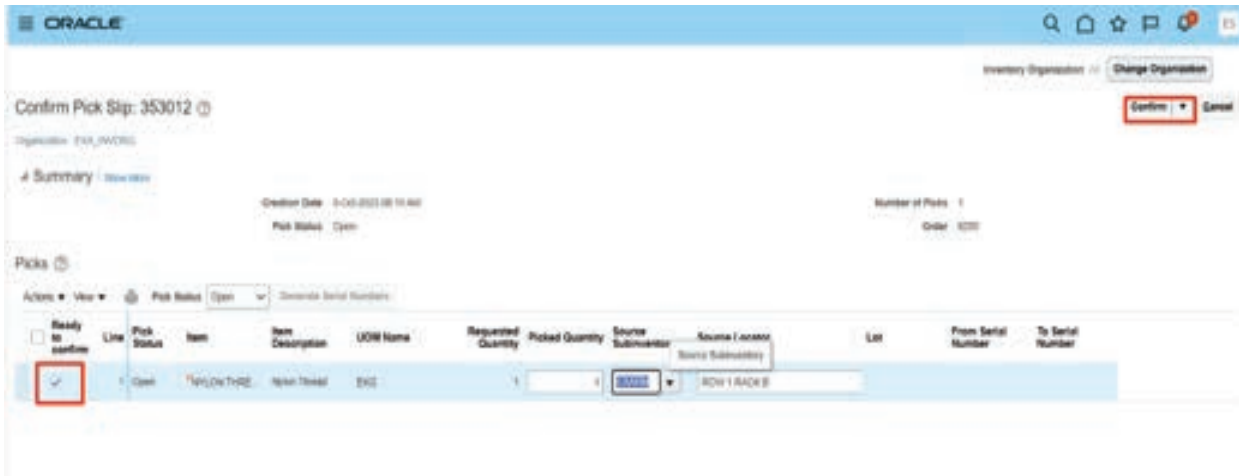
- ii Select the Picks task and click on the Confirm Pick Slips option



- iii Search with the Order number and click on the Pick Slip number



iv Select the line and click on Confirm

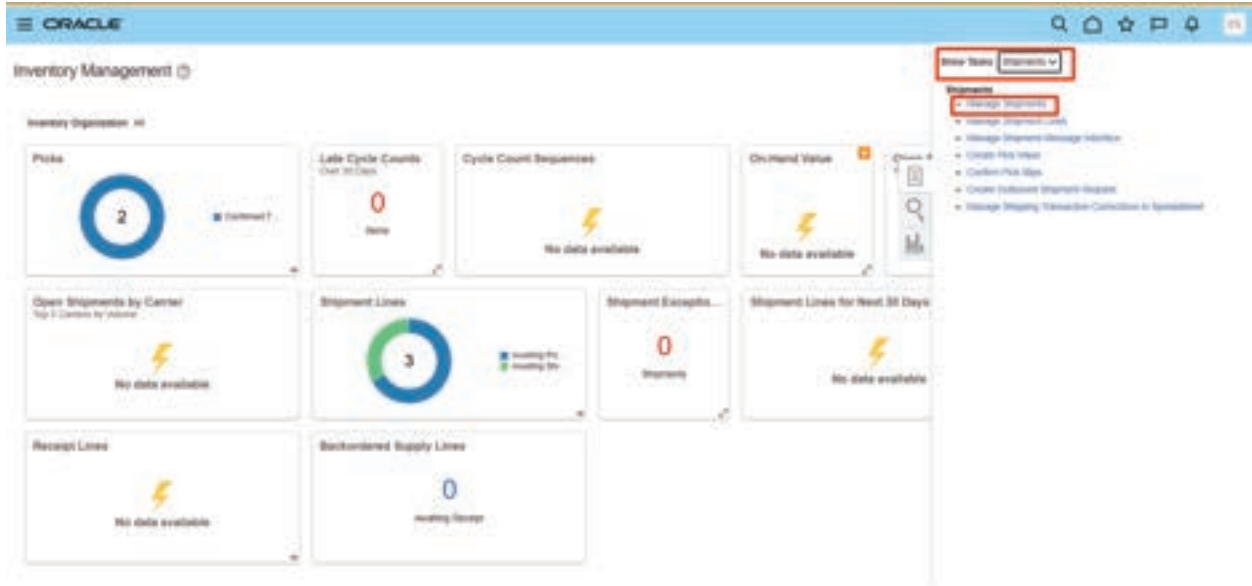


2.2.4 Create ship confirm

i Navigate to Supply Chain Execution > Inventory Management

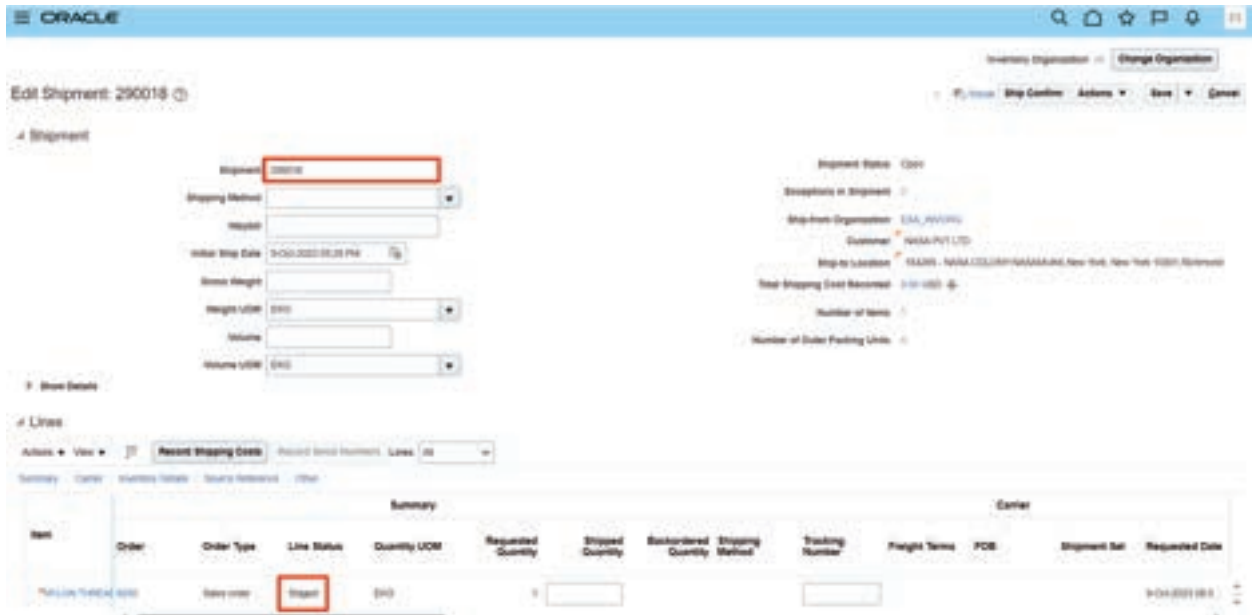


- ii Select the Shipments task and click on the Manage Shipments option



- iii Search with Shipment Number and click on the shipment number link, this number is generated in Pick Slip Report

- iv Shipment line status is changed to Staged.

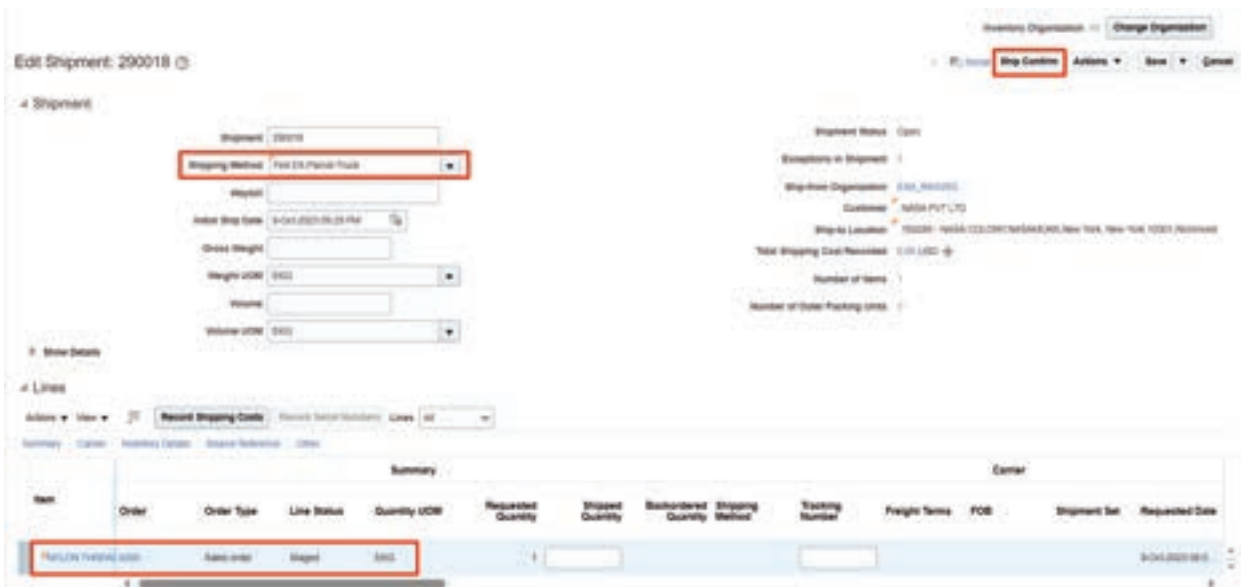


- v And shipment line integration status is Ready to Interface

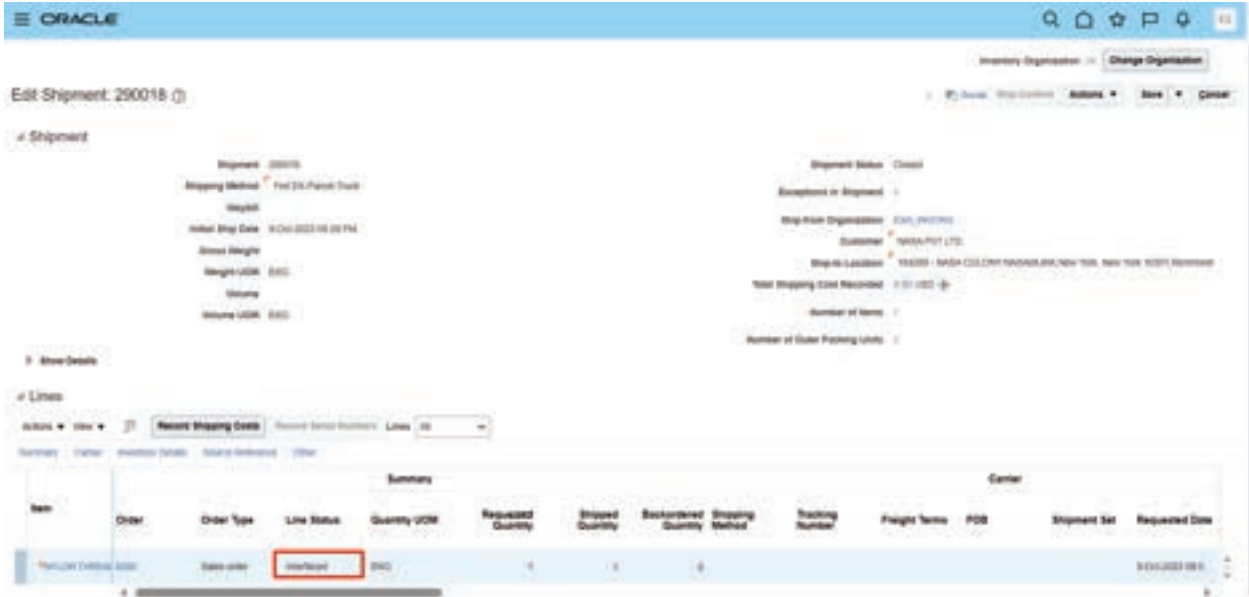


- vi Provide the shipping method and select the shipment line

- vii Click on the ship confirm button



viii Shipment line status will changed to Interfaced



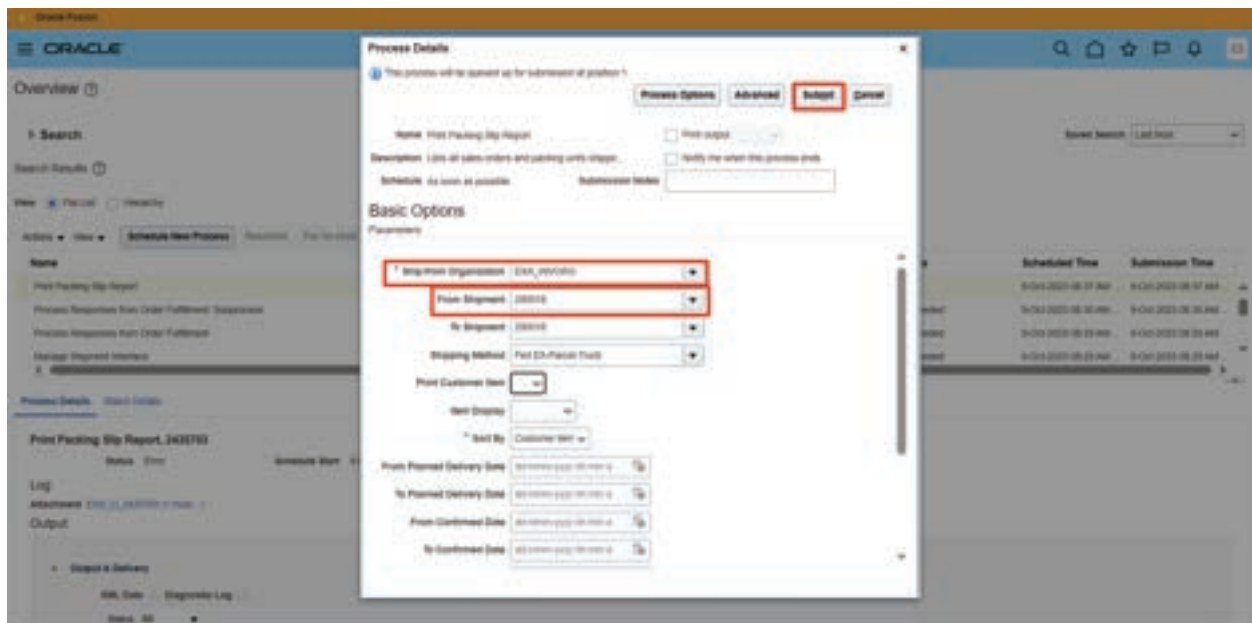
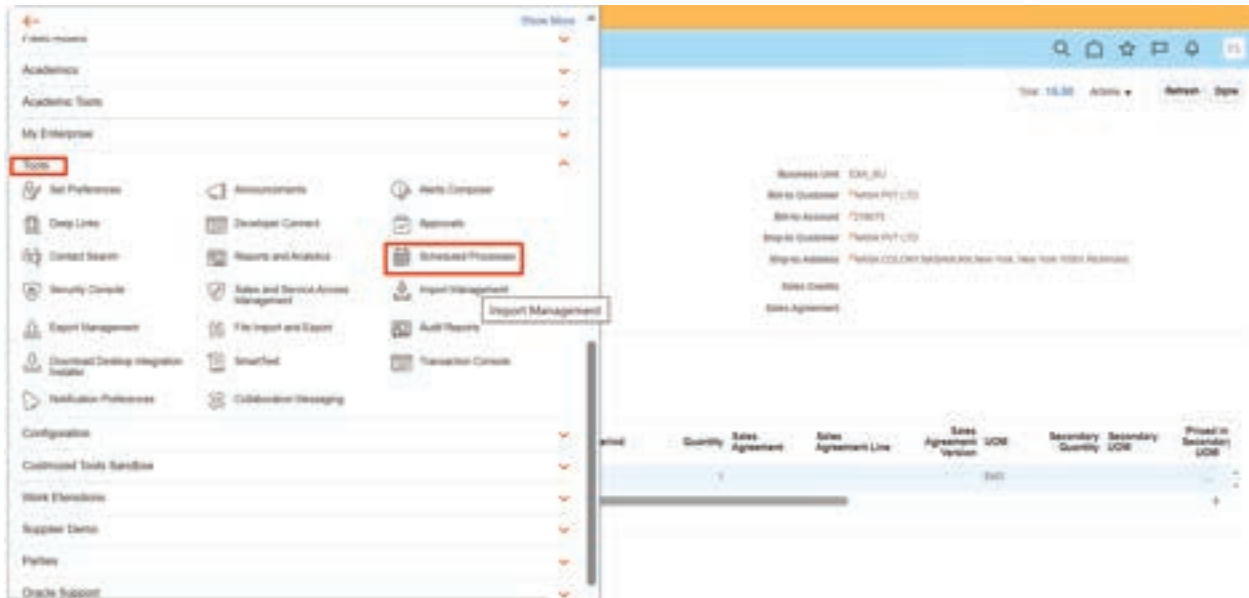
The screenshot shows the Oracle interface for editing a shipment. The top navigation bar includes the Oracle logo and utility icons. The main header displays 'Edit Shipment: 290018'. Below this, there are sections for 'Shipment' details and 'Lines'. The 'Shipment' section includes fields for Shipment ID (29018), Shipping Method (Fed Ex Parcel Truck), Weight, Initial Ship Date (9/24/2023 09:26:14), Gross Weight, Weight UOM (KGS), Volume, and Volume UOM (KGS). The 'Lines' section features a table with columns: Item, Order, Order Type, Line Status, Quantity UOM, Requested Quantity, Shipped Quantity, Backordered Quantity, Shipping Method, Tracking Number, Freight Terms, FOB, Shipment Set, and Requested Date. The first row in the table shows 'THERM TREK-300' with a status of 'Interfaced' highlighted by a red box.

ix Order line status is changed to awaiting billing



The screenshot shows the Oracle interface for editing an order. The top navigation bar includes the Oracle logo and utility icons. The main header displays 'Order: NASA PVT LTD - 6250 - Processing'. Below this, there are sections for 'Summary' and 'Order Lines'. The 'Summary' section includes fields for Customer (NASA PVT LTD (14482)), Contact Method, Ordered Date (9/24/2023 09:26:14), Purchase Order, Order Type (EM BULLSHIP), Business Unit (EM_BU), Bill-to Customer (NASA PVT LTD), Bill-to Account (119115), Ship-to Customer (NASA PVT LTD), Ship-to Address (NASA COLLETH HANDBOOK,New York, New York 10017,NewYork), Sales Credit, and Sales Agreement. The 'Order Lines' section features a table with columns: Item, Status, Duration Period, Quantity, Sales Agreement, Sales Agreement Line, Sales Agreement UOM, Secondary Quantity, Secondary UOM, and Price Secom UOM. The first row in the table shows 'THERM TREK-300' with a status of 'Awaiting Billing'.

x Run Print Packing Slip Report and check the output



Search Results []

View: For List | Refresh

Actions: View | **Schedule New Process** | **Resubmit** | Post-Process | Cancel Process | Archive Process | View Log

Name	Process ID	Status	Scheduled Time	Submission Time
Print Packing Slip Report	2439716	Succeeded	9-Oct-2023 08:29 AM	9-Oct-2023 08:29 AM
Print Packing Slip Report	2439700	Done	9-Oct-2023 08:27 AM	9-Oct-2023 08:27 AM
Process Requested from Order Fulfillment Subprocess	2439670	Succeeded	9-Oct-2023 08:24 AM	9-Oct-2023 08:24 AM
Process Requested from Order Fulfillment	2439668	Not Launched	9-Oct-2023 08:24 AM	9-Oct-2023 08:24 AM

Process Details: **Print Packing Slip Report, 2439716**

Status: Succeeded | Schedule Start: 9-Oct-2023 08:40 AM EDT | External Job Type: PDF Job | External Job Status: OK

Log: Attachment: 1362_2439716

Output

Output & Delivery

Bill, Data, Log, Diagnostic Log | **Attachment 13**

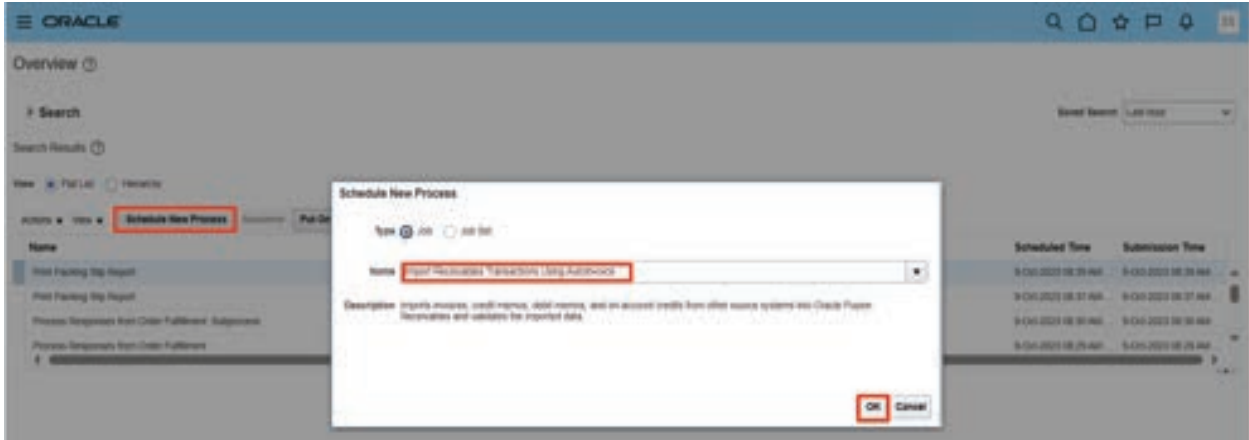
Output Name	Template	Format	Locale	Time Zone	Calendar	Status	Send
Default Document	Packing Slip Report	PDF	English (United States)	UTC (GMT+05:30:30) Standard - Asia (New York)		OK	

ORACLE Packing Slip Date: 9-Oct-2023 08:40 AM
2 Status: Final
Page 2 of 3

Ship From Exacore Inc Org Indeevaran Infopark Kallur Thekkummu, Kerala 680308, India	Customer NASA PVT LTD Ship-to Location NASA COLONY NASAMUKK New York, New York 10301, United States Attention:	Bill To NASA PVT LTD NASA COLONY NASAMUKK New York, New York 10301, United States Attention:
Shipment: 290018 FOB Freight Terms	Tax Number Initial Ship Date: 9-Oct-2023 09:29 PM Shipping Method: Fed EX-Truck-Parcel Waybill	
Transportation Reason		

Order Line	UCM	Requested Quantity	Shipped Quantity
1	EKG	1	1
Secondary Quantity		0	0

xi Run 'Import Receivables Transactions Using Autoinvoice'



xii Verify the Execution Report

ORACLE Vision Operations (USA) Auto Invoice Execution and Validation Report Report Date: 9-Oct-2023 08:52 AM Page 1 of 3

Request ID: 2435762

Transaction Source	Distributed Order Orchestration	From Transaction Number	
Transaction Flexfield		To Transaction Number	
Default Date	9-Oct-2023	From Sales Order Number	6250
Transaction Type		To Sales Order Number	6250
From Customer		From Transaction Date	
To Customer		To Transaction Date	
From Customer Account Number		From Ship-to Customer Account Number	
To Customer Account Number		To Ship-to Customer Account Number	
From Accounting Date		From Ship-to Customer Name	
To Accounting Date		To Ship-to Customer Name	
From Ship Date		Base Due Date on Transaction Date	Yes
To Ship Date		Due Date Adjustment Days	

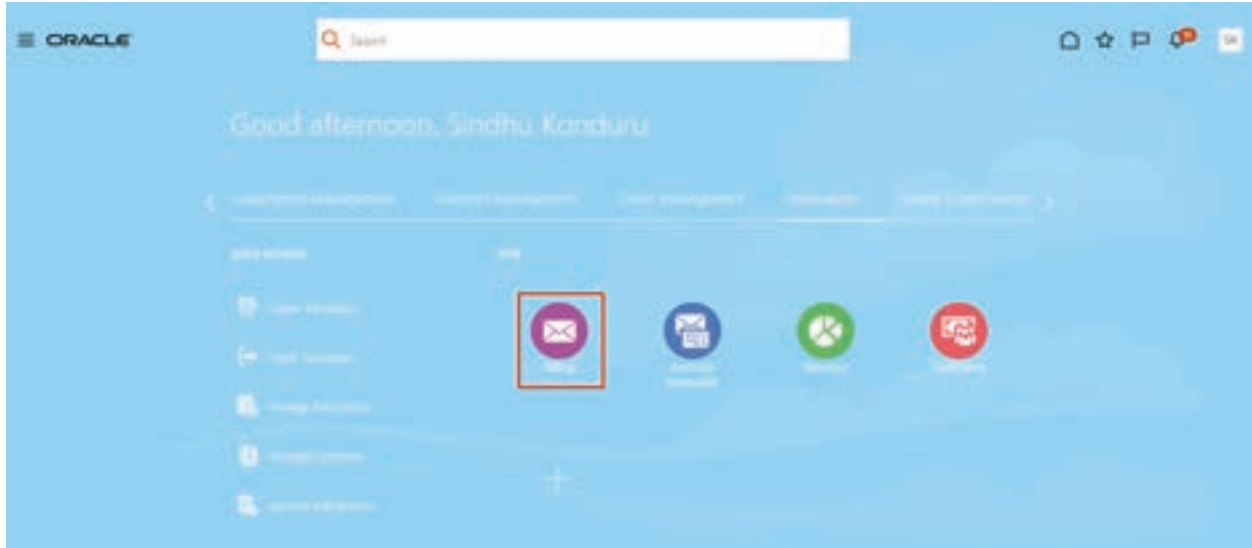
Interface Lines		Interface Distributions	
Selected	1	Selected	0
Successfully Processed	0	Successfully Processed	0
Rejected	0	Rejected	0
Interface Salespersons		Interface Contingencies	
Selected	0	Selected	0
Successfully Processed	0	Successfully Processed	0
Rejected	0	Rejected	0

Rejected Lines by Currency				
Currency	Number of Invoice Lines	Number of Sales Credit Lines	Number of Distribution Lines	Invoice Currency Amount
USD	1	0	0	15.00

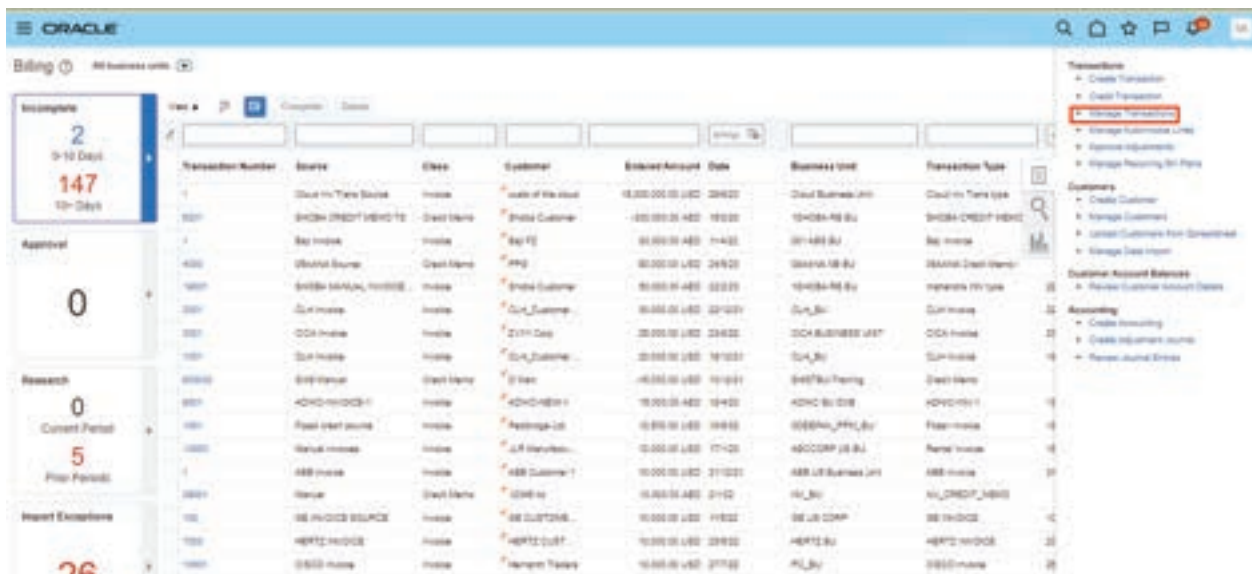
Lines with Errors by Currency				
Currency	Number of Invoice Lines	Number of Sales Credit Lines	Number of Distribution Lines	Invoice Currency Amount
USD	1	0	0	15.00

2.2.5 Verify Transaction (Invoice)

- i Navigate to Receivables > Billing



- ii Click on Manage Transactions in Transactions Task



iii Search with the Transaction Source/Customer Name and the Transaction Number

Manage Transactions

Search

Business Unit: [] Transaction Source: [] Transaction Class: [] Transaction Type: []

Transaction Number: 220102 Transaction Date: [] Bill to Customer: NASSA PVT LTD

Search Reset Save

Transaction Number	Transaction Source	Transaction Class	Transaction Type	Complete	Bill to Customer	Entered Amount	Transaction Date	Business Unit	Original Transaction Number	Service Date From	Service Date To	Invoice Type Code	Inv Sub Type	Pay Max
220102	Manual Invoice	Invoice	INVOICE	Yes	NASSA PVT LTD	15.00 USD	15/03	EUA_BU						

iv Transaction Number is with Complete status and verify the other invoice details

General Information

Business Unit: EUA_BU
Transaction Source: Manual Invoice
Transaction Type: INVOICE
Transaction Number: 220102
Document Number: []

Transaction Date: 15/03
Accounting Date: 15/03
Currency: USD - US Dollar
Transaction Total: 15.00
Line: 15.00
Tax: 0.00
Freight: 0.00
Charge: 0.00

Customer: Bill to Name: NASSA PVT LTD
Bill to Site: 10292
Ship to Name: NASSA PVT LTD
Ship to Site: 10292
Payment Terms: Immediate
Due Date: 15/02

Invoice Details

Line	Item	Description	UOM	Quantity	Unit Price	Amount	Details	Number	Tax Classification	Transaction Business Code
1	NYLON THREAD	Nylon Thread	STD	1	15	15.00	00	6201		Sales Transaction
				Total	1	15.00				

- v To verify balance details, Click on Actions and Click on View Balance Details

Review Transaction: Invoice 2050108

General Information | Show More

Business Unit: EIA_BU
 Transaction Source: Manual Invoice
 Transaction Type: INVOICE
 Transaction Number: 2050108
 Document Number
 Status: Complete

Transaction Date: 9/18/21
 Accounting Date: 9/18/21
 Salesperson:
 Invoicing Rule
 Attachments: None
 Notes:

Customer

Bill-to Name: NASA PVT LTD
 Bill-to Site: 10292

Ship-to Name: NASA PVT LTD
 Ship-to Site: 10429

Payment

Actions | View Image | Save | Incomplete | Cancel

- Credit Transaction
- Submit a Dispute
- Manage Adjustments USD (US Dollar)
- Review Installments 15.00
- Review Deductions 15.00
- Duplicate 0.00
- Post to Ledger
- Account in Draft 0.00
- View Accounting 0.00
- View Balance Details**
- View Transaction Address
- Payment terms: Immediate
- Due Date: 10/5/21

Invoice Details

Invoice Lines | Sales Credits

View | Details

Line Information | Tax Determinants | Revenue Scheduling

Line	Item	Description	UOM	Quantity	Unit Price	Amount	Details	Number	Tax Classification	Transaction Business Code
------	------	-------------	-----	----------	------------	--------	---------	--------	--------------------	---------------------------

Review Transaction: Invoice 2050108

General Information | Show More

Business Unit: EIA_BU
 Transaction Source: Manual Invoice
 Transaction Type: INVOICE
 Transaction Number: 2050108
 Document Number
 Status: Complete

Transaction Date: 9/18/21
 Accounting Date: 9/18/21
 Salesperson:
 Invoicing Rule
 Attachments: None
 Notes:

Customer

Bill-to Name: NASA PVT LTD
 Bill-to Site: 10292

Ship-to Name: NASA PVT LTD
 Ship-to Site: 10429

Payment

Actions | View Image | Save | Incomplete | Cancel

Currency: USD (US Dollar)
 Transaction Total: 15.00
 Lines: 15.00
 Tax: 0.00
 Freight: 0.00
 Charges: 0.00

* Payment Terms: Immediate
 Due Date: 10/5/21

Balance Details: Invoice 2050108

View By: Entered Currency (USD)

Balance Details	Lines	Tax	Freight	Charges	Total
Original amount	15.00	0.00	0.00	0.00	15.00
Receipts	0.00	0.00	0.00	0.00	0.00
Credits/Refunds	0.00	0.00	0.00	0.00	0.00
Adjustments	0.00	0.00	0.00	0.00	0.00
Site Resizable	0.00	0.00	0.00	0.00	0.00
Discounts	0.00	0.00	0.00	0.00	0.00
Balance	15.00	0.00	0.00	0.00	15.00

Sign

- vi To create Accounting for the Transaction
Actions > Post to Ledger



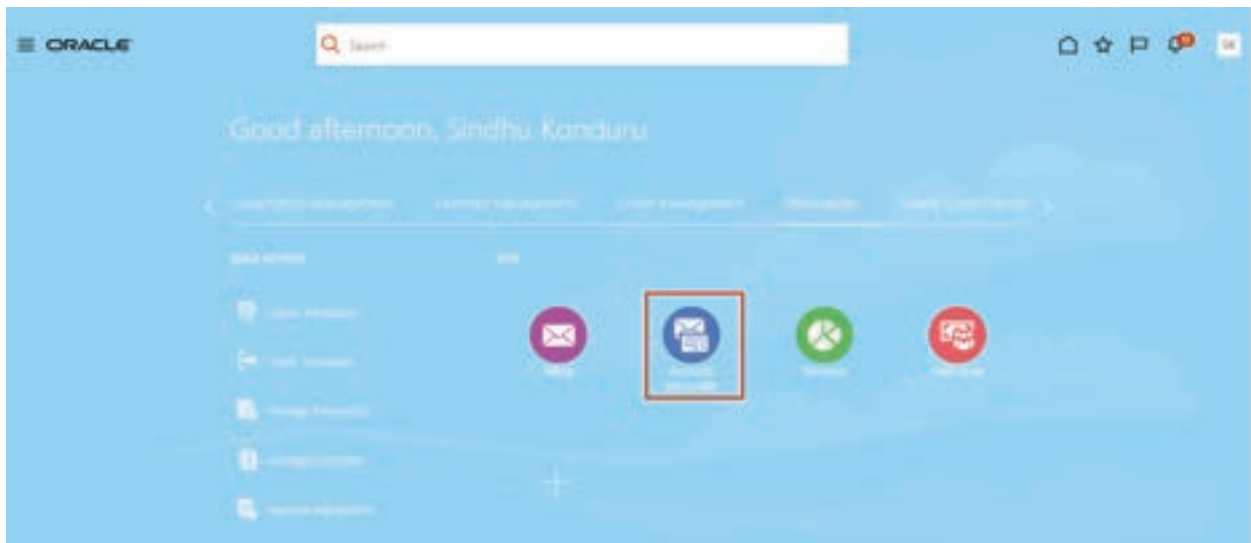
- vii To view the Accounting entry,
Action > View Accounting



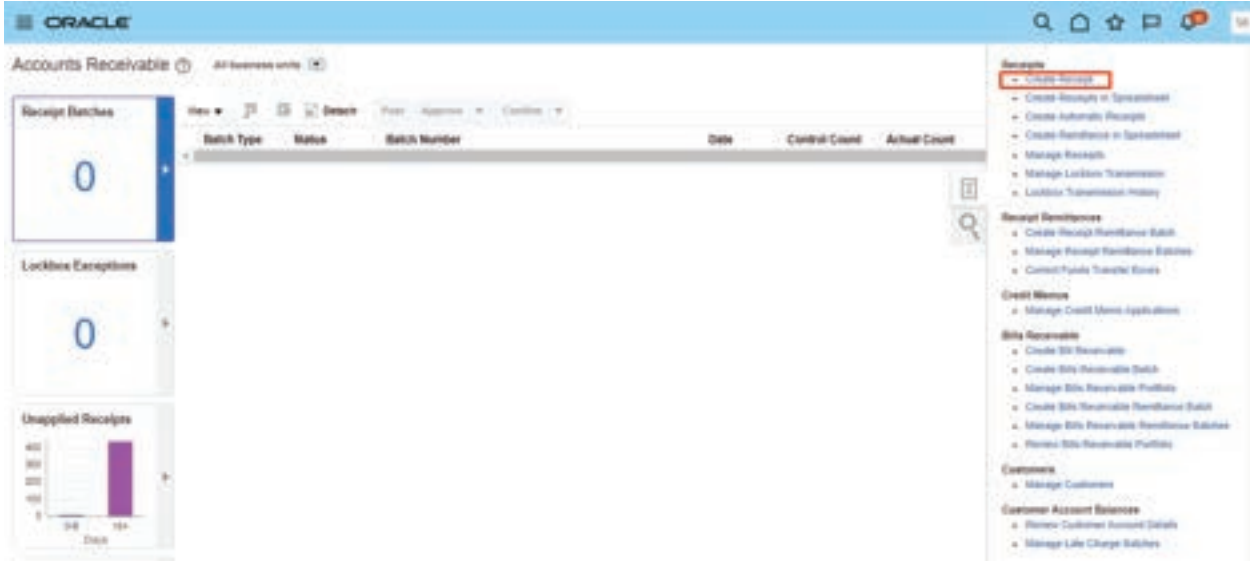


2.2.6 Create Receipt and Apply Transaction (Invoice)

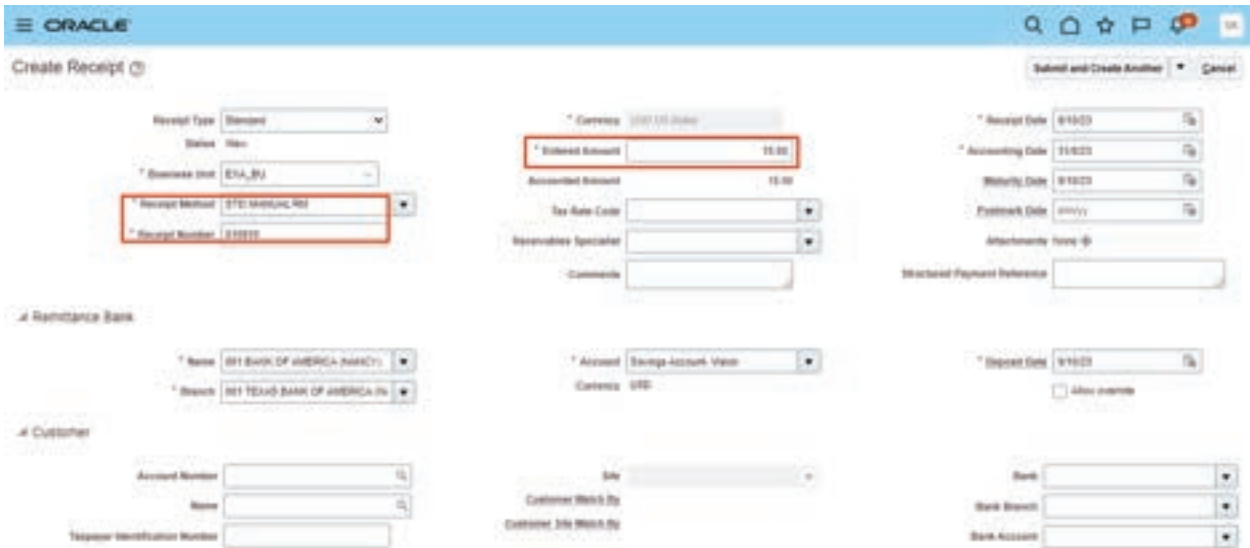
- i Create the Receipt and apply the transaction (Invoice)Number.
Navigate to Receivables > Accounts Receivables



ii Select Create Receipt from Receipts Task



iii Enter the Receipt Method, unique Receipt Number and Receipt Amount



iv Click on Add Open Receivables button to enter the transaction details

The screenshot shows the 'Add Open Receivables' form in Oracle. Key sections include:

- Remittance Bank:** Name (SH BANK OF AMERICA/NANCY), Branch (SH TEXAS BANK OF AMERICA/IN), Account (Savings Account View), Currency (USD), and Deposit Date (3/16/21).
- Customer:** Account Number, Name, Taxpayer Identification Number, Site, Customer Match By, and Bank Account.
- Remittance Reference Detail:** A table with columns 'Receipt Match By', 'Reference Number', and 'Reference Amount'. A red box highlights the 'Add Open Receivables' button above the table.

v Search with Transaction Number or Customer Name

The screenshot shows the search results for 'Add Open Receivables'. The search criteria are:

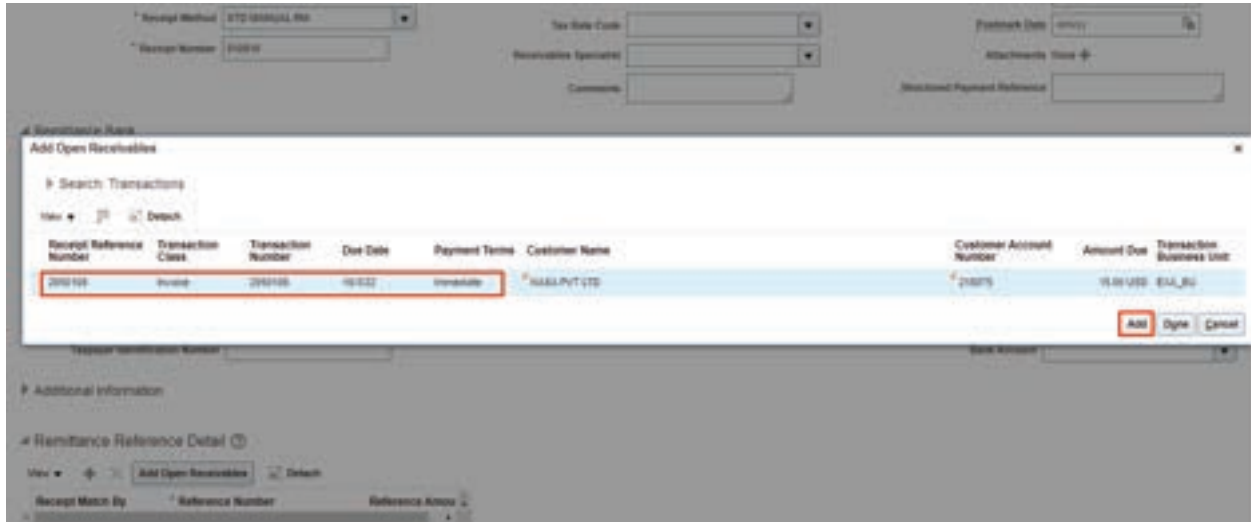
- Receipt Match By: Transaction Number
- Receipt Reference Number: 202100
- Transaction Business Unit: ETA_BU
- Transaction Type: (empty)
- Transaction Customer Name: (empty)
- Transaction Customer Account Number: (empty)
- Currency: (empty)
- Amount: (empty)
- From Transaction Due Date: (empty)
- To Transaction Due Date: (empty)

Search filters on the right include:

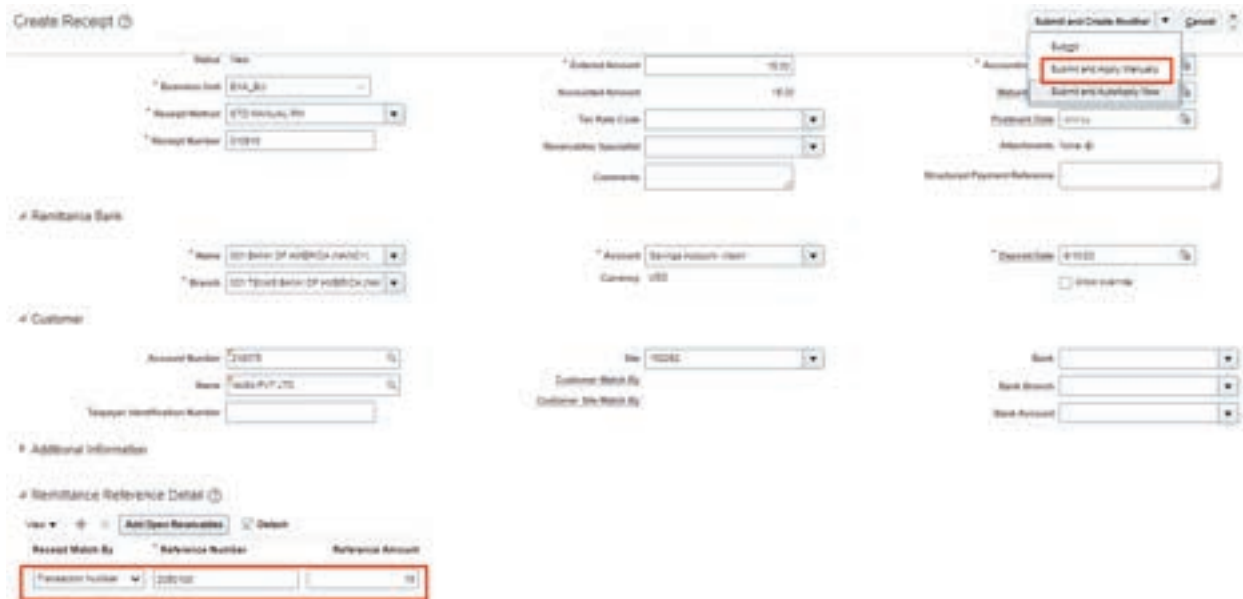
- Include Inactive Customers
- Include Cross Currency Transactions
- Include Disputed Transactions
- Include Closed Transactions
- Include Chargebacks
- Include Draft Items
- Include Draft Items
- Include Bill Receivable
- Include Internal Transactions Excluded from Collections

The table below the search criteria has columns: Receipt Reference Number, Transaction Class, Transaction Number, Due Date, Payment Terms, Customer Name, Customer Account Number, Amount Due, and Transaction Business Unit. A red box highlights the 'Search' button.

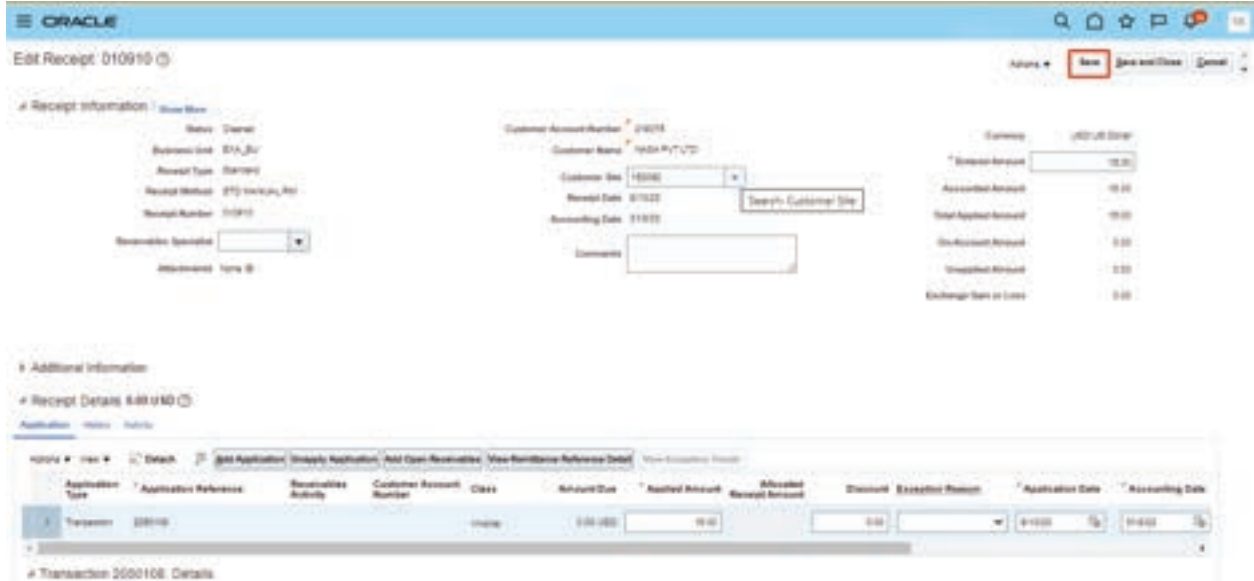
- vi Select the Transaction line
- vii Click on Add > Done



- viii Click on Submit and Apply Manually



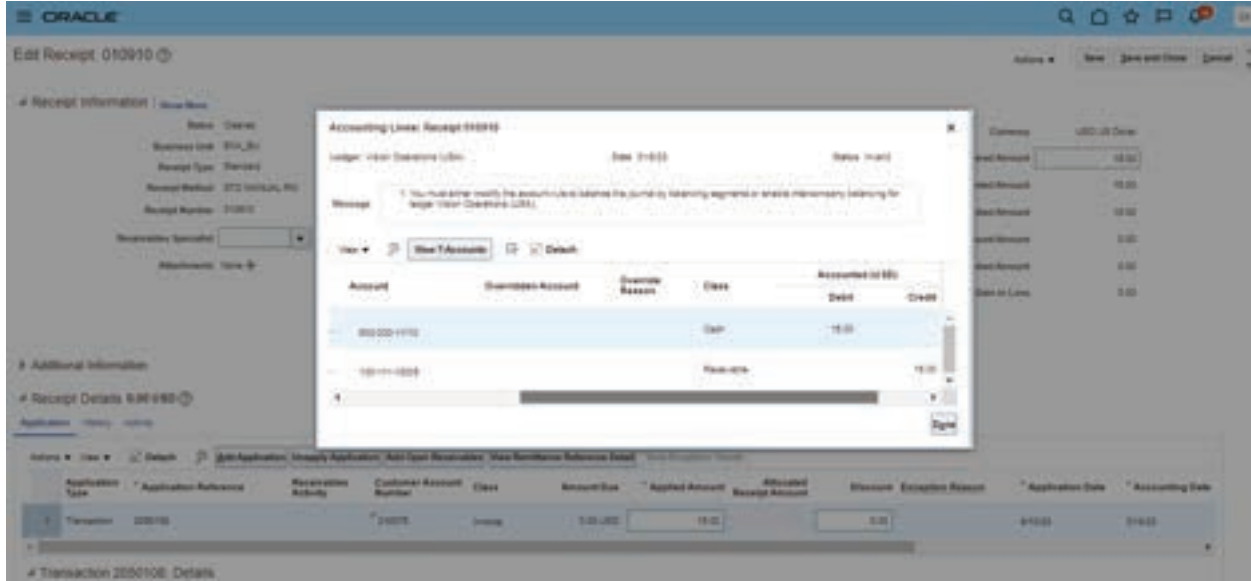
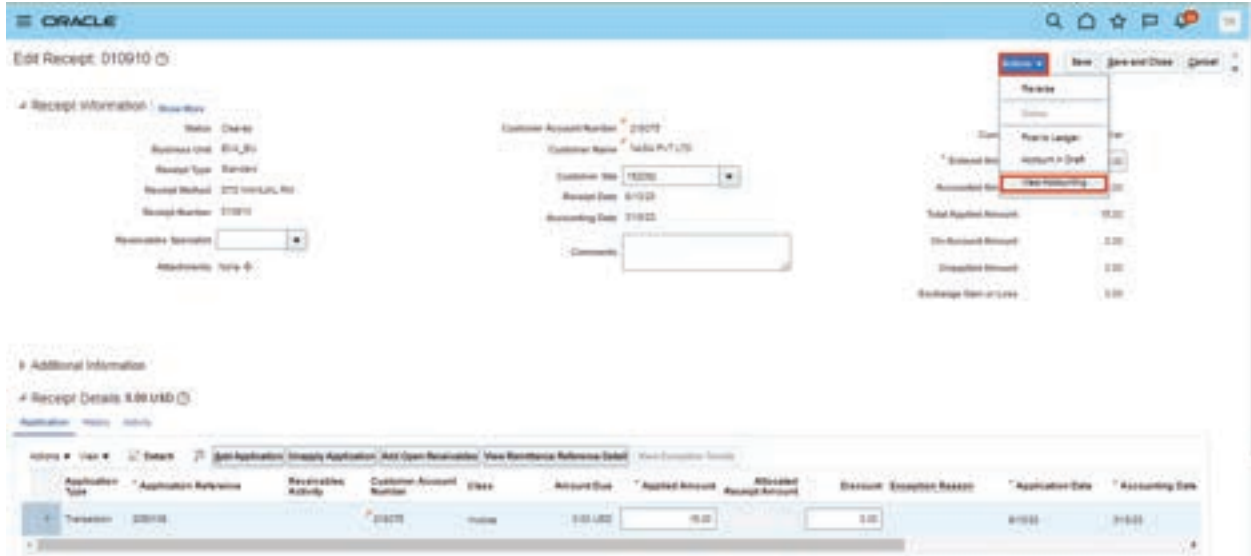
ix Click on Save



x To create Accounting for the Receipt
Actions > Post to Ledger



- xi To View the Accounting Entry
Actions > View Accounting



2.3 O2C REPORTS

2.3.1 Collections Aging 4 Bucket Report

Using collections aging reports user can list customer's open transactions information which can help in creating collection strategies and tasks. User can view customer's open transactions based on the aging buckets defined.



ORACLE Vision Operations (USA)		Aging - 4 Bucket Report					Report Date	7/3/14 2:34 PM
							Page	1 of 1
Customer Name	Customer Number	Outstanding Amount (USD)	Current Current (USD)	1-30 days past (USD)	31-60 days past (USD)	61+ days past (USD)		
A T & T SOLUTIONS INC	1001	998,386,603,307.11	96,884.63	0.00	0.00	998,357,306,793.05		
			.00%	.00%	.00%	100.00%		
	Customer Receipts At Risk	0.00						
	Customer Balance	998,386,603,307.11						
Imaging Innovations, Inc.	1002	9,927,707.71	0.00	0.00	0.00	9,927,707.71		
			.00%	.00%	.00%	100.00%		
	Customer Receipts At Risk	0.00						
	Customer Balance	9,927,707.71						
UNITED PARCEL SERVICE, INC	1003	673,023.45	0.00	0.00	0.00	673,023.45		
			.00%	.00%	.00%	100.00%		
	Customer Receipts At Risk	0.00						
	Customer Balance	673,023.45						
	Total for All Customers	998,397,204,030.27	96,884.63	0.00	0.00	998,407,906,324.21		
			.00%	.00%	.00%	100.00%		
	Total Receipts At Risk	0.00						
		0.00						

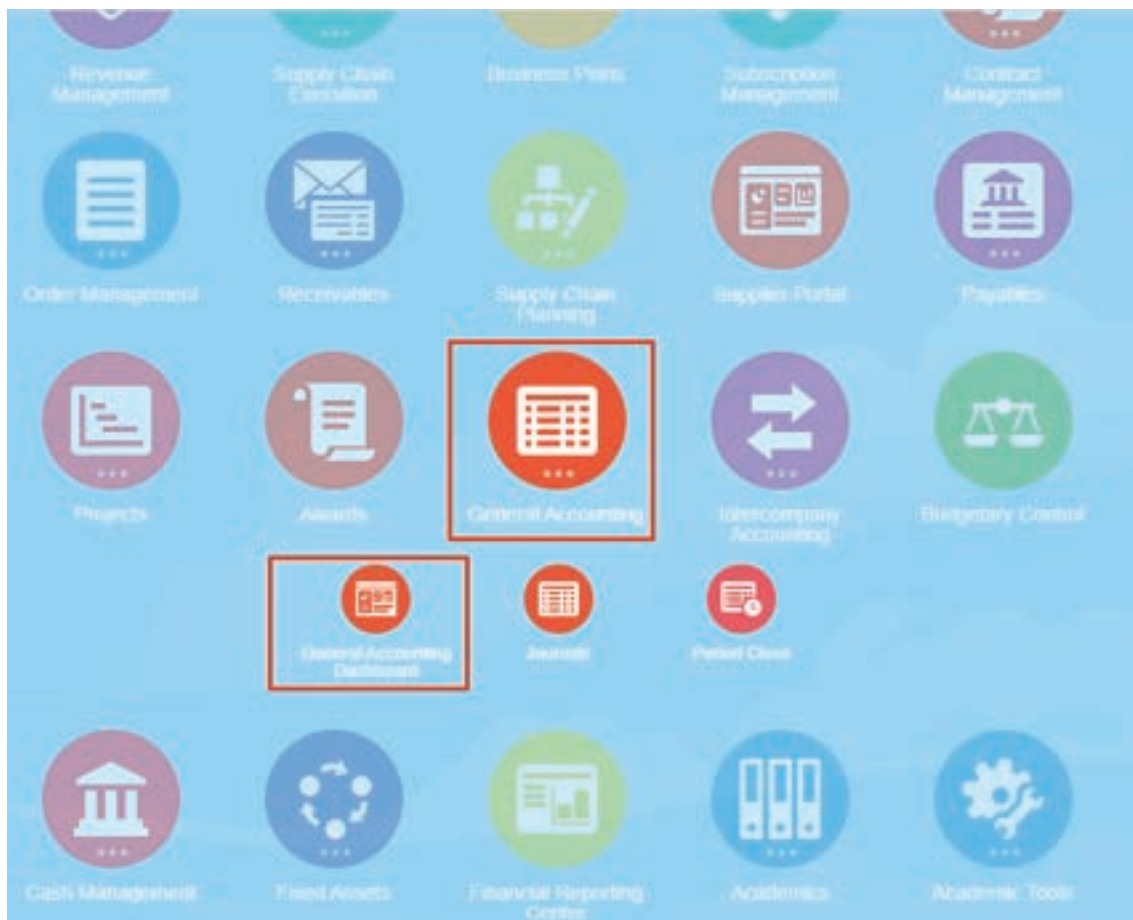
2.4 INQUIRE ON DETAIL BALANCES

Run account inquiries using the Inquire on Detail Balances page. To get to the page, select the Inquire on Detail Balances task in the Period Close work area.

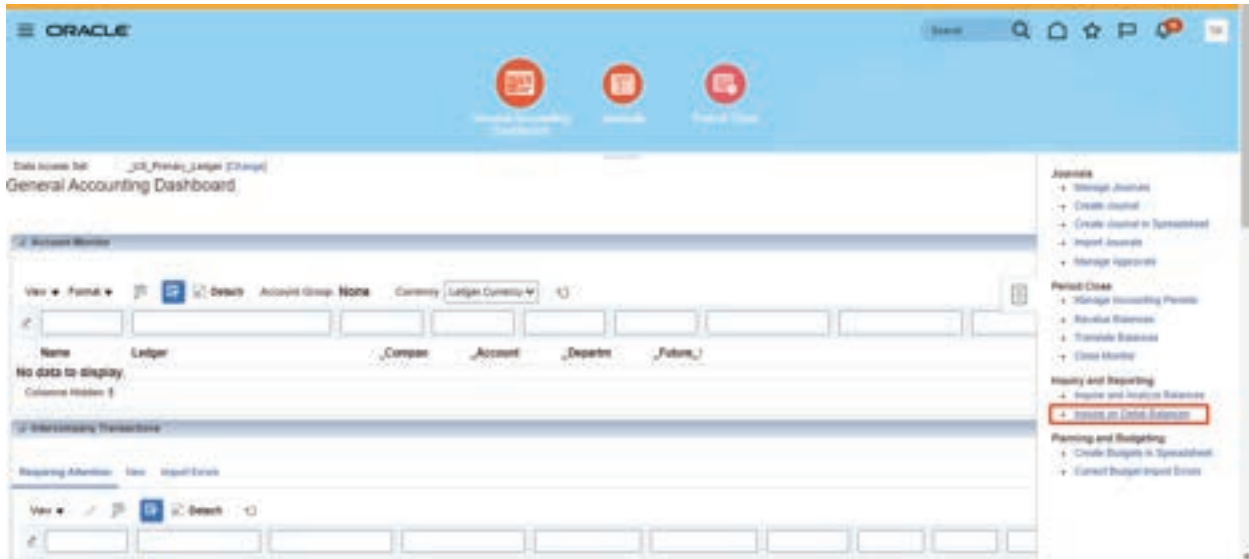
Account inquiry helps to :

- Drill to journal lines for actual balances and then drill to the journal entry or subledger transactions.
- Export the balances to Excel

i Navigate to : Home > General Accounting > General Accounting Dashboard

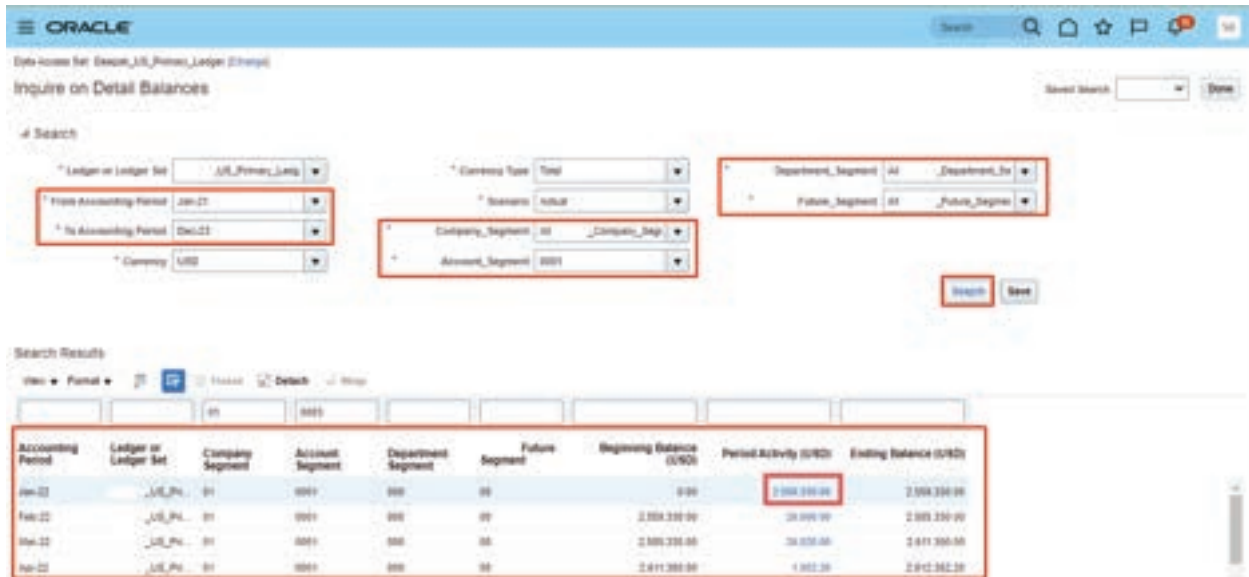


ii Task > click Inquire on Detail Balances



iii Enter the Accounting period and Account segment values and click on search.

iv In the search results click on the period activity for the required month to check the transactions in details.



ORACLE

Data Access Set: _JRT_Primary_Ledger

Journal Lines: 01.0001.000.00

Ledger: _JRT_Primary_Ledger
Account Description: Retail Company CASH AC Defult Defult

View: Format: [Grid] [Tree] [Details] [Map]

Journal Batch	Journal	Line	Accounting Date	Source	Category	Entered		Accounted (USD)	
						Debit	Credit	Debit	Credit
		1	4/1/02	Manual	Adjustment	100.00 USD		100.00	
		1	4/1/02	Spreadsheet	Adjustment		1,800.00 USD		1,800.00
		1	4/1/02	Manual	Adjustment	150.00 USD		150.00	
		1	4/1/02	Manual	Adjustment	300.00 USD		300.00	
		1	4/1/02	Spreadsheet	Adjustment	1,000.00 USD		1,000.00	

CHAPTER 3

FUSION - AUDIT

A business object's specific attributes can be tracked in an audit's modification history. However, the application's auditing must be enabled for that application, and those objects and their characteristics must be chosen for audit.

The properties to audit for a particular item and the timing of the audit depend on your configuration choices. All actions taken, including create, update, and delete, on an object and its attributes are considered during an audit.

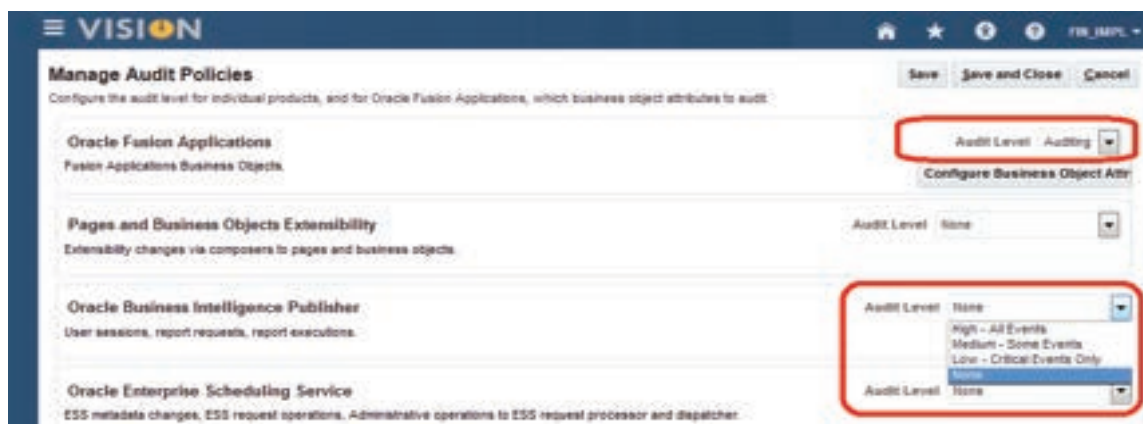
3.1 TURNING ON AUDITING IN FUSION APPLICATIONS

Prior to choosing which business objects to audit, you must enable auditing.

The auditing option in the application is not turned on by default.

Go to the Manage Audit Policies page in the Setup and Maintenance work area to configure the attributes of audit business object.

- 1 Open **Setup and Maintenance** work area (also known as Functional setup Manager).
- 2 Search on **Manage Audit Policies** and click the link to open the Manage Audit Policies page.
- 3 For Oracle Fusion Applications Audit Level, select **Auditing**.
- 4 You can also enable auditing at specific levels for other items.

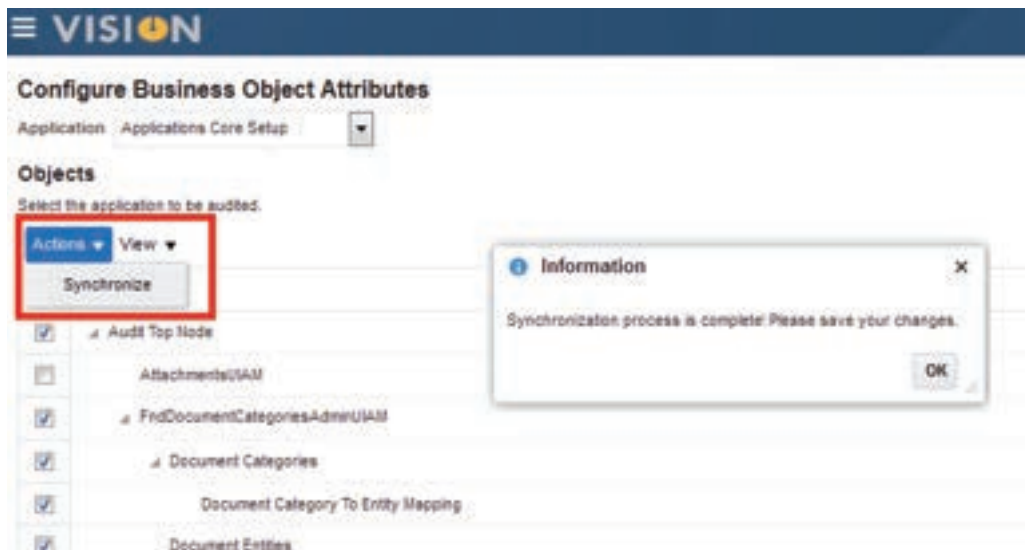


3.1.1 OPTIONS FOR BI PUBLISHER

- 1 To select specific products to audit, select the **Configure Business Object Attribute** button. This will open the Configure Business Object Attributes page.
- 2 Select the Application dropdown to see all products you can enable.
- 3 You can also enable auditing for specific Financials products, such as Payables and Receivables.

3.1.2 OPTIONS FOR APPLICATIONS CORE SETUP

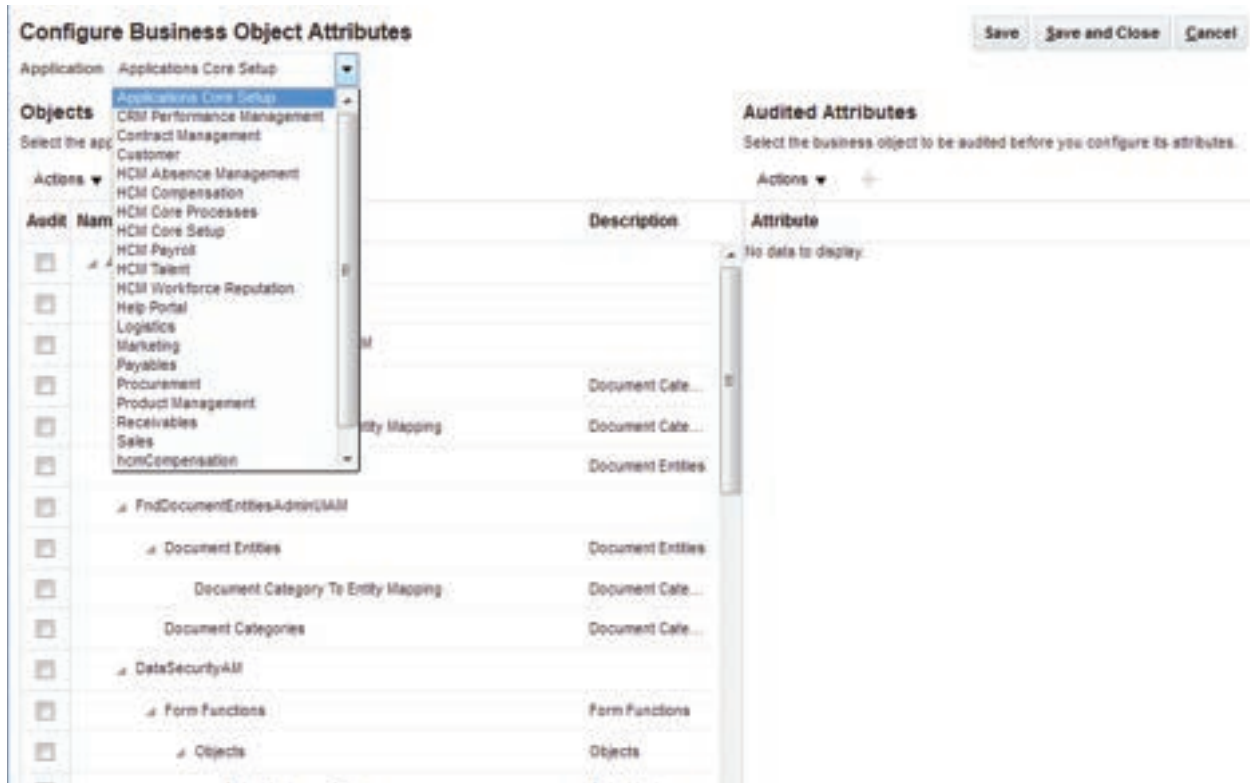
- 1 For the Applications Core Setup, by selecting the Audit Top Node check box, it will enable auditing for everything.
- 2 Then click **Actions > Synchronize**.



Note: The synchronization process is carried out by product in order to complete the enablement of auditing.

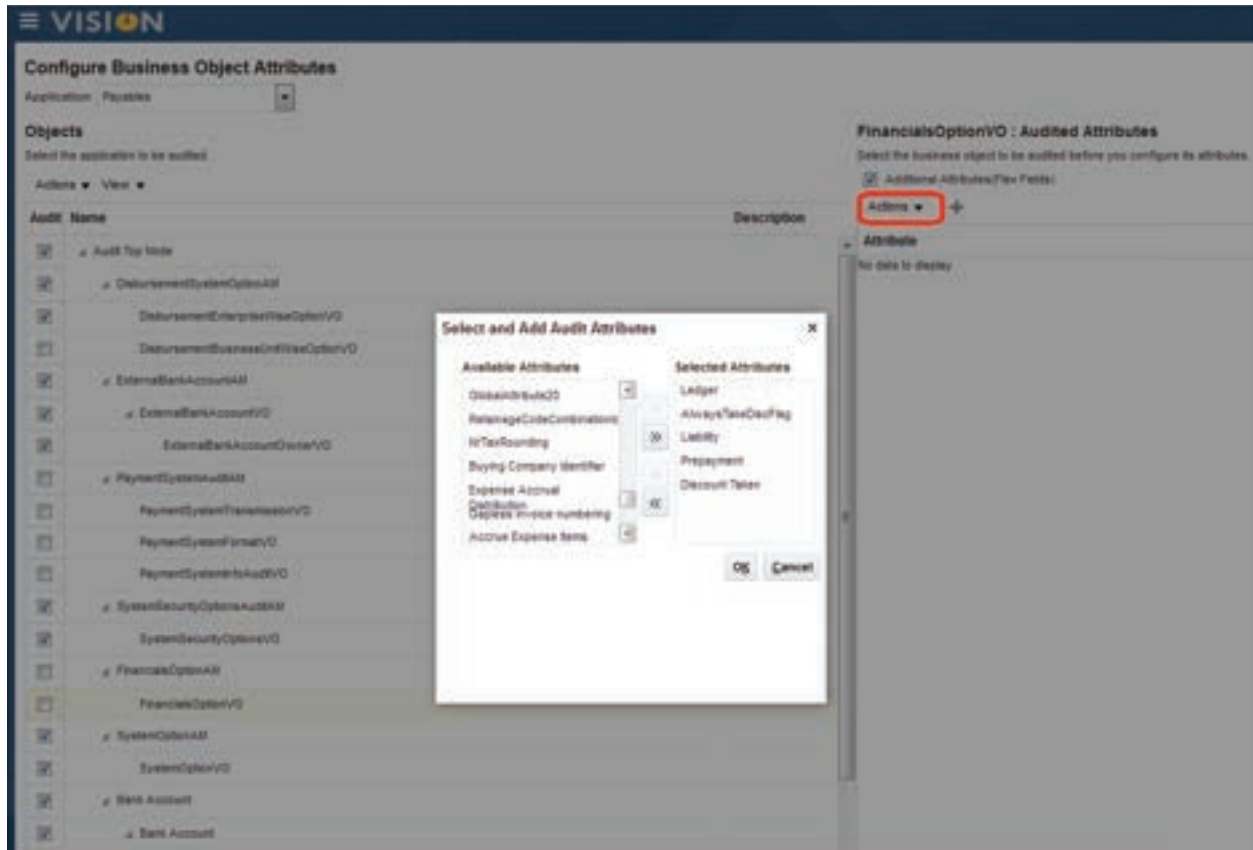
Flex field attributes (chart of account values) are always included by default, so with these you want to be sure to do a synchronization. On a patch or update, or if attributes have been added, they must be tracked if they are meant to be included in the audit. Synchronize will do this.

- Click **Save** or **Save and Close**.



3.2 Auditing for Payables

- After selecting the Audit Top Node check box, you will notice that some business objects are not checked. For example, the Financials OptionVO. This is because you have to select the attributes associated to that business object that you want to audit.
- By selecting the Financials OptionVO row, click Actions > Create, it will open the Select and Add Audit Attributes popup.
- Move attributes from the Available Attributes box to the Selected Attributes box. You probably want to just blindly select everything. The Payables financials options VO relates to the Manage Common Options for Payables and Procurement setup page, which is an important setup page.



Note: Additional Attributes (Flex Fields) – Flex Fields (chart of account combinations) can be audited just by selecting this checkbox.

- Click **Actions > Synchronize**.
- Click **OK > Save and Close > Save and Close**.

Repeat this process for other business objects and other products.

3.3 VERIFYING AUDIT CONFIGURATION

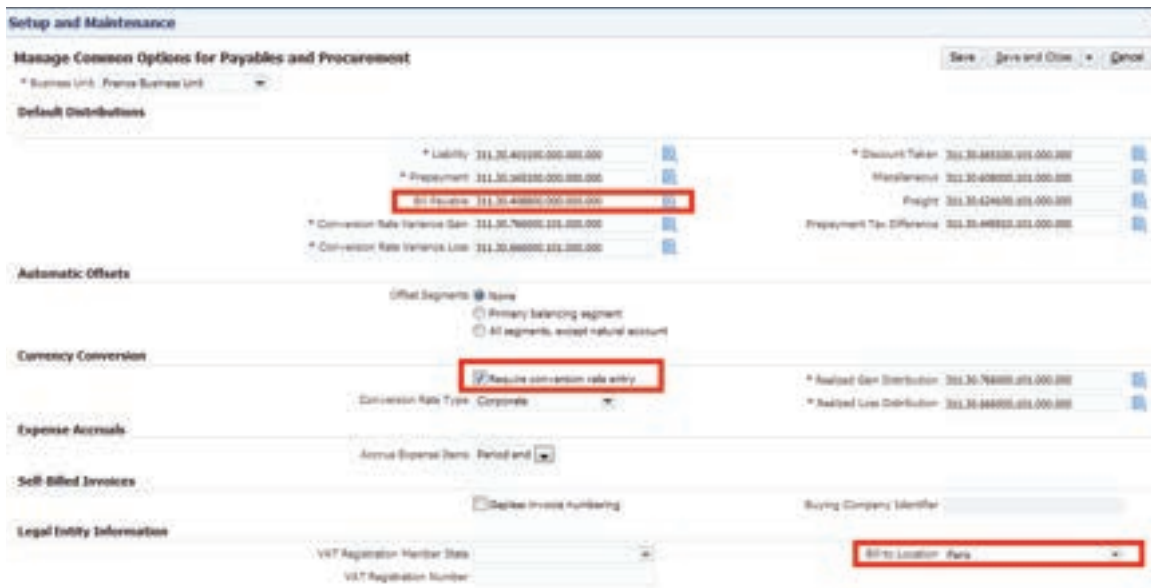
3.3.1 OPTIONS FOR PAYABLES AND PROCUREMENT

To test the auditing setup made to the Manage Common Options for Payables and Procurement setup page (related to the Payables Financials Options VO) perform the following

- 1 Login as a different user.
- 2 Open the Setup and Maintenance work area.
- 3 Query task **Manage Common Options for Payables and Procurement** and click the link to open the page.
- 4 Select the Business Unit and then change accounts and other options.

In this example, following has been changed

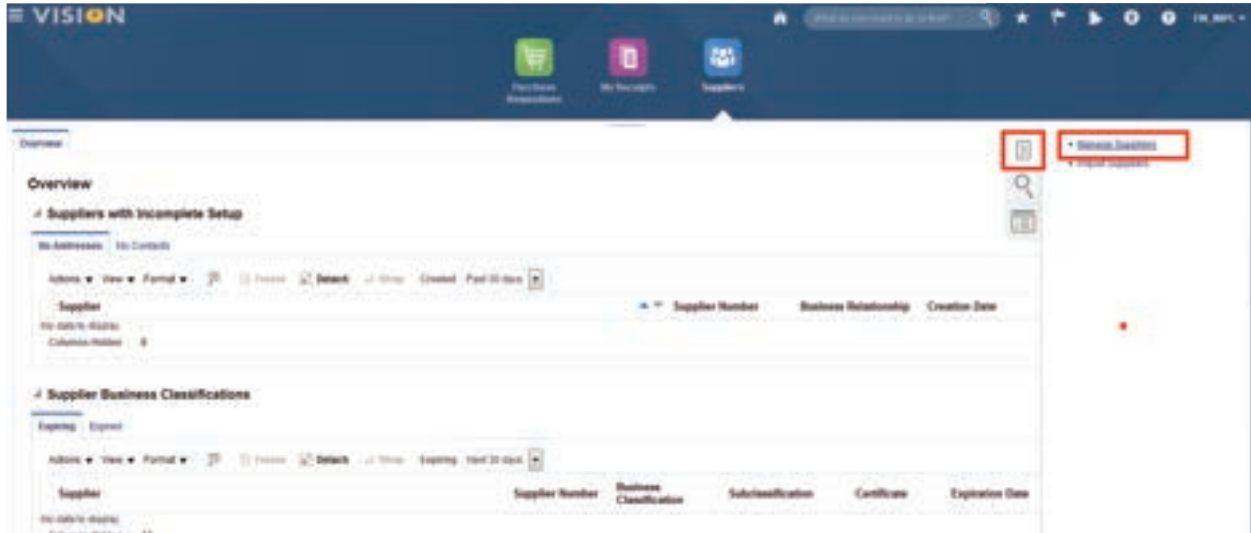
- o Bills Payable Account (Changed the account)
- o Require conversion rate entry (Enabled)
- o Bill-To Location. (Added Bill to Location)



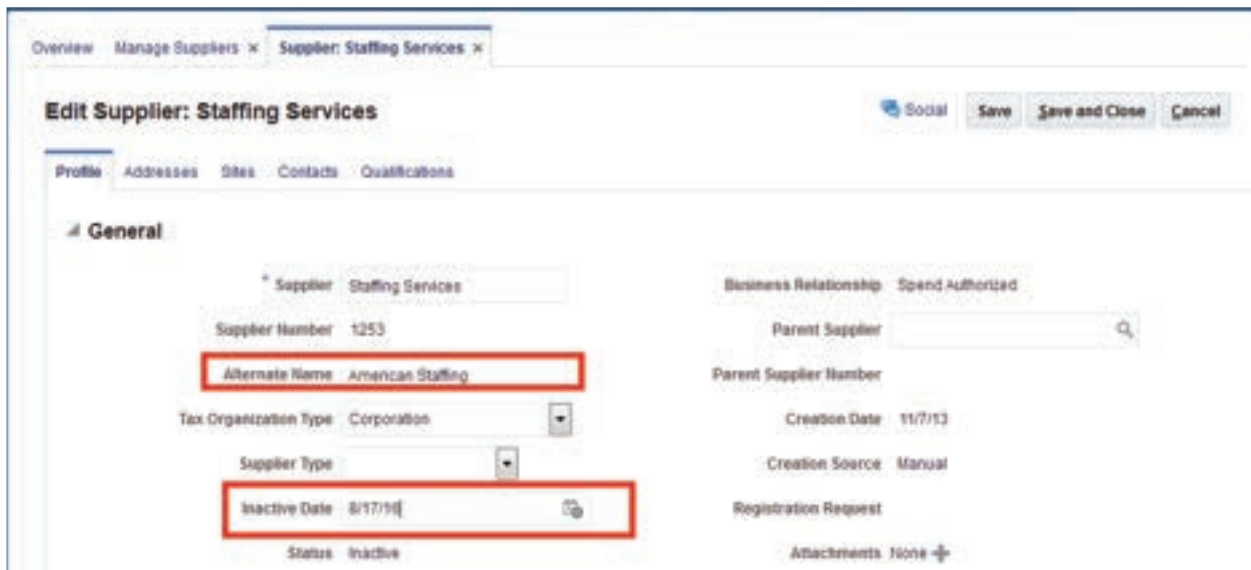
Click **Save and Close**.

3.3.2 UPDATE AN EXISTING SUPPLIER

- i Open the Manage Suppliers page.
(Navigator > Procurement>Suppliers, click task “Manage Suppliers.”)



- ii From the Manage Suppliers page, search for an existing supplier.
- iii In this example, an Alternate Name and an Inactive Date has been added.
(logged in as a different user called Casey.Brown).



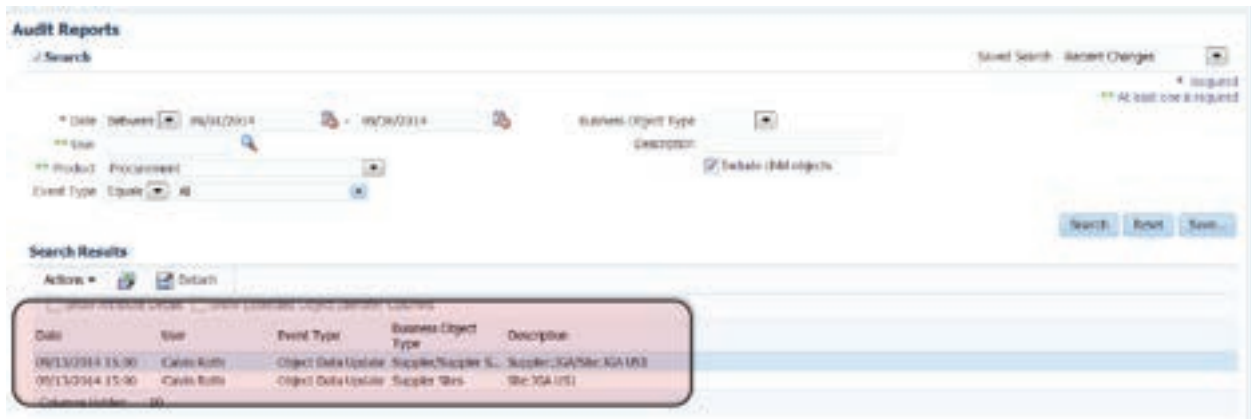
Click **Save and Close**.

3.4 AUDIT REPORTS

- i Open the Audit Reports page (Navigator > Tools > Audit Reports)
- ii Specify your search criteria, such as the Date Range (Required), User, Product, Business Object Type, etc.



- iii Click the Search button.
- iv You can then view the results in the Search Results table and export the results to Excel.



UNIT

5

MS DYNAMICS

CHAPTER 1

EXPLORE THE CORE CAPABILITIES OF MICROSOFT DYNAMICS 365 FINANCE AND OPERATIONS APPS



LEARNING OBJECTIVES

- Describe enterprise resource planning (ERP).
- Describe use cases for finance and operations apps.
- Describe the finance and operations apps user interfaces.

DESCRIBE THE FINANCE AND OPERATIONS APPS

1.1. INTRODUCTION

This module discusses the general capabilities of the Microsoft Dynamics 365 suite of finance and operations apps, including use cases and descriptions of the user interfaces.

1.2. DESCRIBE ENTERPRISE RESOURCE PLANNING (ERP)

Enterprise resource planning (ERP) is business process management software that manages and integrates a company's financials, supply chain, operations, reporting, manufacturing, and human resource activities. Fundamentally, ERP software enables you to run the core processes of a business.

Generally, ERP software consists of a set of integrated business functions that automate back-office processes including procurement, inventory management, and assembly. Organizations can gain a real-time view across their operations by using one central database. The following illustration depicts business functions supported by an ERP system.

A diagram that shows business functions supported by an ERP system. Such as General ledger, Project accounting, Procurement and sourcing, and Inventory management.

An effective ERP system allows an organization to analyze transactional data, resulting in more streamlined processes and greater efficiency.

Introducing Dynamics 365:

Dynamics 365 is a set of intelligent business applications that work together seamlessly. It provides customer relationship management (CRM) opportunities for marketing, customer service, field service, and sales through its customer engagement apps. Dynamics 365 also covers operations, finance, commerce, and human resources through its finance and

operations apps. Dynamics 365 combines CRM and ERP capabilities by bringing them together in a powerful set of applications and moving them to the cloud. Although CRM and customer engagement apps are an important part of the Dynamics 365 suite of applications, this module focuses on ERP and finance and operations apps.

Dynamics 365 connects with Microsoft Power Platform and Microsoft Dataverse for insights, innovation, and connectivity between your data and your business processes. Dynamics 365 consists of transactional applications, like Business Central, and finance and operations applications that help your organization automate processes and increase efficiency.

Finance and operations apps help businesses manage their global financial systems, operational business processes, and streamlined supply chains to empower people to make fast, informed decisions.



Finance and operations apps:

Dynamics 365 Finance helps you redefine your traditional global financial management to monitor performance in real time, predict future outcomes, and make data-driven decisions to drive business growth. You can automate processes to manage financial complexities, increase efficiency, and decrease operational expenses.

Dynamics 365 Supply Chain Management empowers employees and organizations with the ability to obtain a unified view of inventory, warehouse, manufacturing, service, and logistics with predictive analytics that turn data into insights to support better strategic decisions. It brings agility and efficiency to manufacturing by connecting and optimizing production planning, scheduling, operations, and cost management. It gives you real-time visibility into warehousing and transportation business processes to reduce costs, reduce delivery time, and increase accuracy.

Dynamics 365 Commerce delivers a comprehensive solution that unifies your back-office, in-store, call center, and digital experiences. Commerce enables you to build brand loyalty through personalized customer engagements, increase revenue with improved employee productivity, and optimize operations to reduce costs and drive supply chain efficiency, delivering better business outcomes.

Dynamics 365 Human Resources provides the workforce insights you need to build data-driven employee experience. Human Resources can improve organizational agility, optimize programs, discover workforce insights, and transform employee experiences. Your human resources team can centralize personnel data, automate processes, and enable self-service.

Dynamics 365 Project Operations provides the visibility, collaboration, and agility needed to drive success across the project-centric business—from prospects to payments to profits. It connects sales, resourcing, project management, and finance teams in a single application to win more deals, accelerate project delivery, and maximize profitability.



Microsoft Dynamics 365 Business Central

Dynamics 365 Business Central:

Dynamics 365 provides a business management solution named Business Central for small and mid-sized organizations. Business Central automates and streamlines business processes within areas such as finance, manufacturing, sales, shipping, project management, and services. Finance and operations apps, however, provide an enterprise solution targeted to complex organizations.

There are several other important differences between Business Central and finance and operations apps. Business Central can be implemented for a single user, whereas finance and operations apps require a minimum of 20 users for implementation. Business Central is also an all-in-one solution, whereas finance and operations apps allow you to choose which functionalities you want to add. In addition, Business Central has built-in customer relationship management (CRM) functionalities, whereas finance and operations apps need to integrate with customer engagement apps to implement CRM functionalities.

1.3. DESCRIBE FINANCE AND OPERATIONS APPS USE CASES

Why use finance and operations apps?

You're starting to realize the limitations of your current ERP system and are considering an upgrade to something new and modern. It might be time to replace your existing ERP system and implement new software like Dynamics 365 if you have:

- Lack of capacity
- Lack of insights
- An existing system that is costly to operate

Lack of capacity:

Problem: Your current system hasn't kept up with you as your company has grown and added more staff, clients, and business processes or entered new lines of business or markets.

Solution: An ERP solution allows your company to expand while the solution manages your company's everyday business processes.

Lack of insights:

Problem: Even though ERP software offers real-time visibility of your entire business, and insights into the industry landscape, your company still uses software that works independently from other systems. This can lead to different departments working in silos.

Solution: Finance and operations apps offer data analytics and business insights by connecting all the disparate systems together and provides a win-win solution by offering productivity, growth, and a competitive edge.

An existing system that is costly to operate:

Problem: You pay a lot to operate your current ERP deployment. You may not know the pros and cons that come with each deployment option, whether it's on-premises, in the cloud, or a hosted ERP solution.

Solution: It may be time for an even closer look to decide if you should move to the cloud, keep things on-premises, or invest in a combination of both.

Discover what a modern ERP system can offer:

Dynamics 365 scales with your business as you expand into other markets and helps keep client and company data secure. Additionally, it extends your everyday processes as you grow.

The resource planning tools that Dynamics 365 applications offer can help you:

- Increase productivity.
- Get control of financial management.
- Help with human resources management.
- Streamline project management needs.
- Improve supply chain and operations management.
- Make better decisions by using business intelligence and artificial intelligence (AI).

Cloud vs. on-premises implementation of finance and operations apps:

You can deploy finance and operations apps in the cloud or on-premises. Cloud deployments offer an ERP service that is fully managed by Microsoft, while on-premises deployments are deployed locally within a customer's datacentre.

The following table provides a comparison of the capabilities provided by the two deployment options.

Capability	Cloud	On-premises
Infrastructure and data location	- Cloud service managed by Microsoft - Datacenters managed by Microsoft	- Infrastructure managed by customer or partner - Disconnected datacenter - Local data residency
Data trustee	- Microsoft	- Customer
Application lifecycle management (ALM)	- Managed by Microsoft - Customer access ALM and telemetry using Dynamics 365 Lifecycle Services	- Managed by customer or partner with cloud-based ALM and telemetry using Lifecycle Services
Cloud capabilities	- High availability and disaster recovery included	- High availability and disaster recovery managed by customer or partner

1.4. DESCRIBE THE FINANCE AND OPERATIONS APPS USER INTERFACES

Finance and operations apps include several categorizations of user interface (UI) elements, including navigation, controls, and filters.

Navigation pane:

The leftmost pane of the finance and operations apps is called the navigation pane, from which you can access any page. The following options are in the navigation pane:

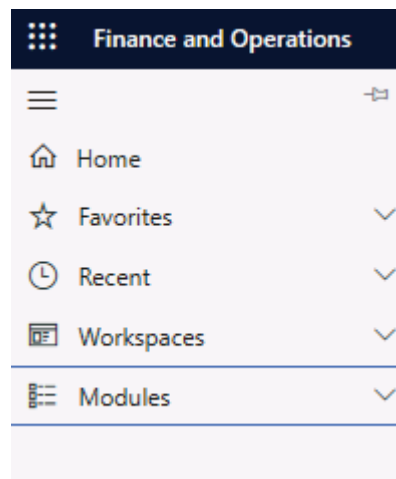


Figure 1.1. Navigation pane.

- **Favorites:** You can mark and then select your most frequently used pages for easy navigation to these pages.
- **Recent:** Your recently opened pages are automatically saved under the Recent menu.
- **Workspaces:** All the workspaces are available in finance and operations apps under the Workspaces menu. Workspaces provide the option to create personalized dashboards for users based on their job profile and activities.
- **Modules:** You can find all the modules, sub-menus, and pages under the Modules menu.

Navigation bar:

The uppermost title bar of the finance and operations apps is called the navigation bar. The following screenshot displays the options in the navigation bar:



Figure 1.2. Navigation bar with descriptions of some of the icons: Go to Office 365, Search for a page, Company picker, Show message, and Settings.

Go to Office 365:

The waffle icon in the upper-left corner of the navigation bar takes you to the Office 365 portal, a cloud-powered, subscription-based productivity platform. From the portal, you can access apps, including Microsoft Teams, Word, Excel, PowerPoint, Outlook, and OneDrive.

Search for a page:

When you type the name of a page in the search box, all the pages with a similar name appear in the list along with the navigation path, as in the example in the following screenshot. You can navigate directly to the required page.

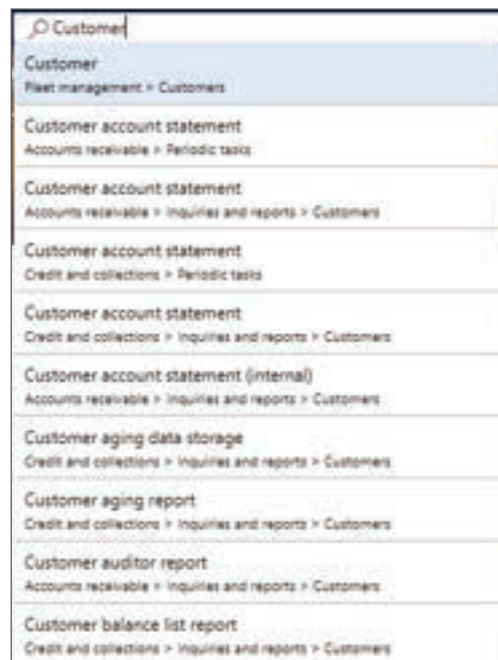


Figure 1.3. Results of a search for the Customer page in the search box.

Company picker:

The Company picker option allows you to select a legal entity. All operations and transactions in the finance and operations apps pertain to the selected legal entity. Legal entities are described in more detail in the Explore use cases for legal entities unit in the “Learn the fundamentals of Microsoft Dynamics 365 Finance” learning path.

Show messages:

The Show messages option opens the Action center, which has all the system messages generated in the finance and operations apps.

Settings:

The Settings option has several features, depicted in the following screenshot, that users can configure based on their business requirements and preferences.

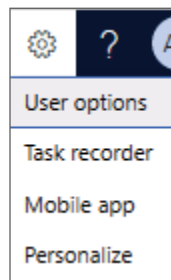


Figure 1.4. Features available under the Settings option.

User options:

This option helps you set up user-specific configurations. The User options page has four tabs.

Visual:

The first tab is named Visual, depicted in the following screenshot, from which a user can define the general color and size of all the interfaces of the finance and operation apps.

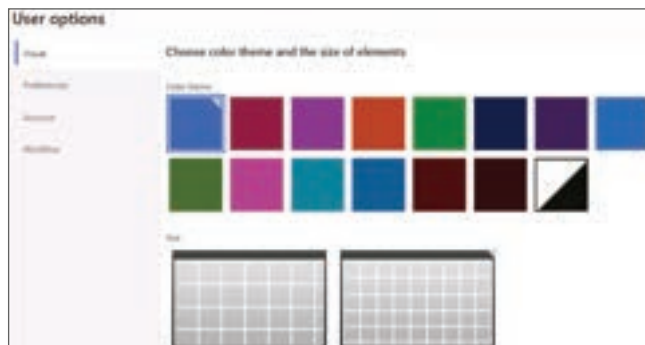


Figure 1.5. Visual tab of the User options page.

Preferences:

In the Preferences tab, you can define user-specific configurations, including location and language. The Preferences tab has five Fast Tabs, depicted in the screenshot:

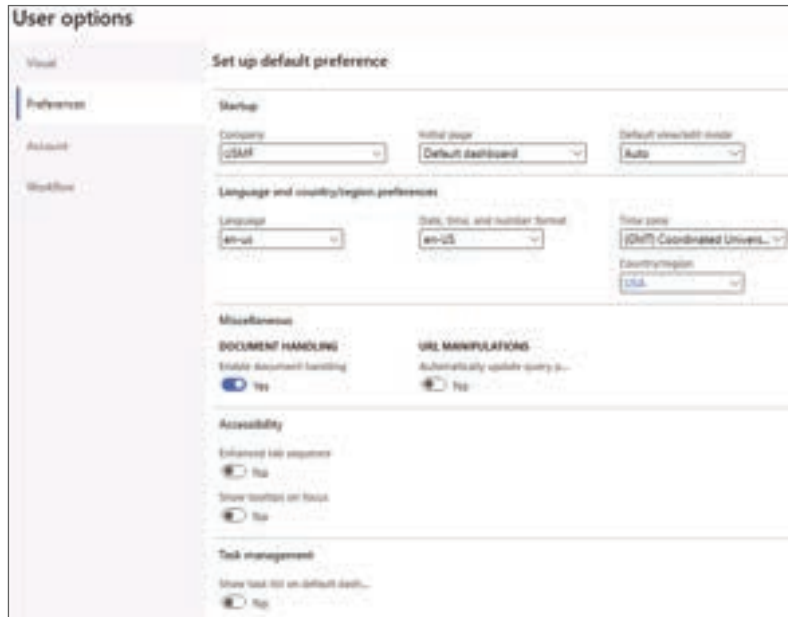


Figure 1.6. Preferences tab of the User options page.

- **Startup:** In the Start up Fast Tab, you can define which legal entity to open when finance and operations apps are opened. You can also define which default dashboard to open during startup.
- **Language and country/region preferences:** In the Language and country//region preferences Fast Tab, you can define your default country//region and the time zone in which you're working. You can also define the date, time, and number format of your region. You can define the language you want in the labels. Changes to any of these values immediately change the respective configurations for you in the finance and operations apps.
- **Miscellaneous:** In the Miscellaneous Fast Tab, you can enable the Document handling feature, which associates documents, images, and notes with the records entered into the finance and operations apps. For example, you can associate a brochure for and photo of a new product that you have added in the finance and operations apps.
- **Accessibility:** In the Accessibility Fast Tab, you can enable the Enhanced tab sequence field. This ensures that all page elements are in the tab sequence. The only exceptions are elements that have been explicitly marked as not being in the tab sequence through personalization. The Show tooltips on focus field ensures that when a control receives focus, the tooltip for that control displays automatically to the user.

- **Task management:** In the Task management Fast Tab, you can enable a task list on the default dashboard.

Account:

The Account tab, depicted in the following screenshot, depicts the user credentials along with the email provider and email ID of the user. It allows you to send mail directly from the finance and operations app. Users can also enable electronic signature in this tab.

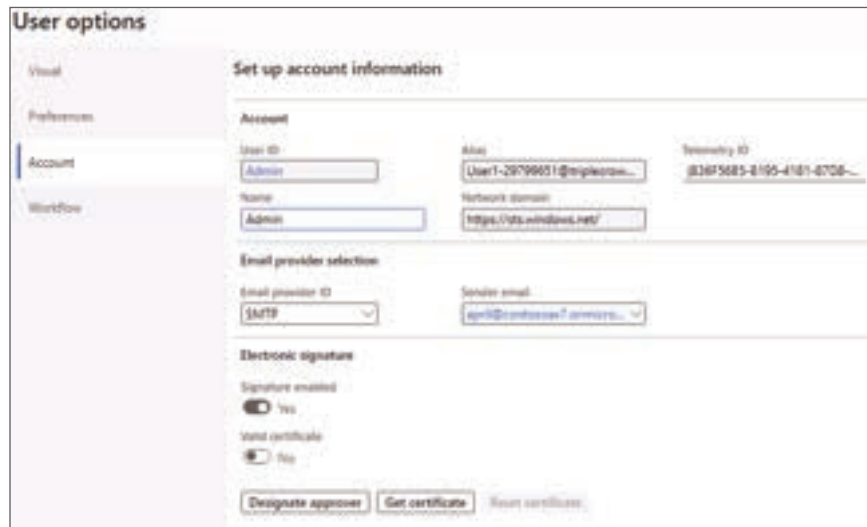


Figure 1.7.Account tab.

Workflow:

In finance and operations apps, there's a standard workflow framework that can be associated with different business processes. For example, during the different stages of an ongoing workflow, you might need to send an email for notification purposes. In the Workflow tab, depicted in the following screenshot, you can configure the mailing options. You can also define the delegation options to delegate workflow approval authority during your absence.



Figure 1.8.Workflow tab in the User options page.

Task recorder:

This feature is a utility in finance and operations apps that allows users to record business processes for different use cases, including the following:

- Step-by-step guided tours of specific business processes in the application
- Documentation of a business process as a Microsoft Word document that can optionally include screenshots
- Regression tests for a business process
- Automatic playback of a business process in the application

Once the business processes are recorded, they can be saved in the following ways:

- Save to this PC
- Save to Lifecycle services
- Export as Word document
- Save as developer recording

Save to this PC:

The task recording package can be saved as an .axtr file and uploaded in the business process modeler (BPM) tool in Lifecycle Services. The .axtr file creates the test case for the business process.

Save to Lifecycle services:

You can directly save a recorded task to Lifecycle Services corresponding to a business process in BPM. The task is automatically stored as a test case for the business process. The test case is also be reflected in the Microsoft Azure DevOps instance connected to the Lifecycle Services project.

One of the major uses of task recorder is Regression Suite Automation Tool (RSAT). This tool facilitates regression testing and significantly reduces the time and cost of the user acceptance test (UAT). RSAT is fully integrated with DevOps for executing, reporting, and investigating test cases. The task recordings that are uploaded into DevOps as test cases can be run seamlessly in the RSAT tool. This helps the business process owner to automate the testing of the business process configuration and customization. The test data is stored in Excel, which is decoupled from the test steps.

Export as Word document:

The recorded tasks can be saved as a Word document. This is mostly used when a user is looking for a user manual or use case document based on a real example.

Save as developer recording:

This option helps you to generate XML files from the task recorder. You can import the XML recordings to generate test code that can be used to validate business process scenarios. Generated code is based on the Sys Test Framework and Form Adaptors, which facilitate unit/component testing. You can also import the XML recordings in the Performance software development kit (SDK) tools to perform multiuser load testing.

Mobile app:

The mobile app can enable the business processes of finance and operations apps in mobile devices. Your IT admin needs to publish mobile workspace for the devices. Users can then use the mobile workspace to perform business actions. Standard workspaces are already available, and users can create custom workspaces and add actionable forms in them. The following screenshot depicts some of the standard mobile workspaces available in the app.

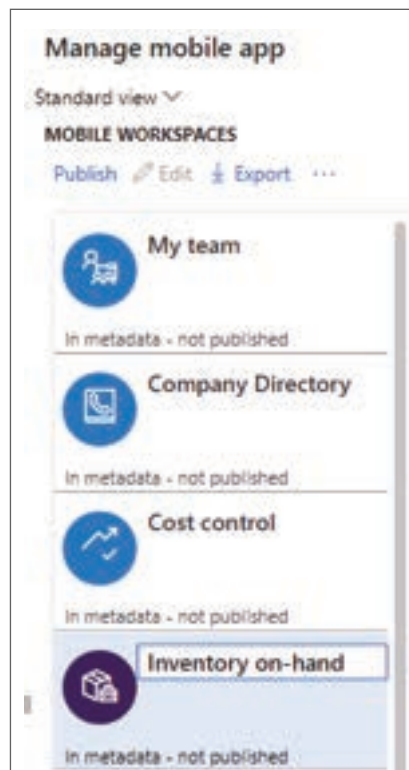


Figure 1.1.9. Standard mobile workspaces in the mobile app.

Personalize:

Personalize options, depicted in the following screenshot, enable you to make changes in the UI, including adding a field in a page, making a field mandatory, and moving the position of a field. The changes are visible only to the user who made them.

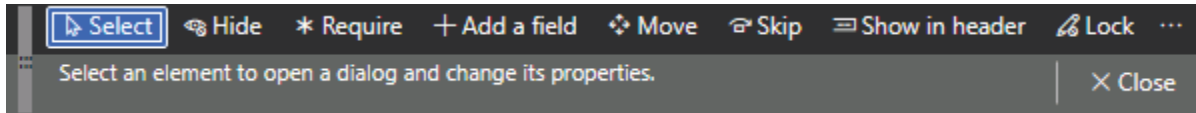


Figure 1.1.10. User-specific personalization.

Action Pane:

The Action Pane is a control on a page. When you open a page, for example, the Customer page in the following screenshot, the topmost section of the page is the Action Pane.

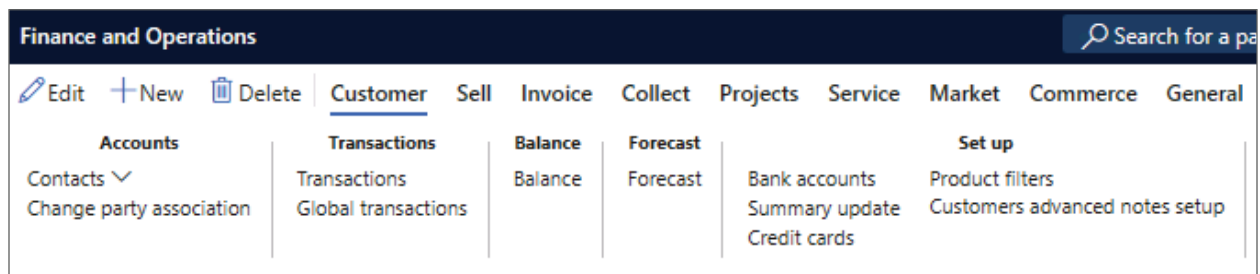


Figure 1.1.11. Customer page of the action pane.

The basic actions on a page, such as creating, editing, deleting, and saving records, are performed by the buttons in the Action Pane. In addition to the Edit, New, and Delete buttons, the Action Pane may have other buttons that perform business scenarios related to the Customer page, such as customer balance, customer bank account, and forecast.

Filters:

Finance and operations apps offer four filtering options in the pages:

- Quick filter: This is a filtering mechanism that appears above any list or grid and provides fast single-column filtering.
- Filter pane: This is an inline pane that slides in from the left and contains multiple filter criteria that can be applied to the targeted content.
- Grid-column filter: This enables you to define filter conditions and perform single-column sorting by using a drop-dialog control that is opened from the grid column header.
- Advanced filter or sort: This provides an advanced filter and sort capability based on multiple columns. This filtering option is available under the Options button in the Action Pane.

Filtering and sorting in Dynamics 365:

These filtering and sorting techniques are applicable to most of the pages in the finance and operations apps.

Workspaces:

A workspace is a one-stop shop for specific activities. Think of workspaces as personalized work centers with data, reports, and transactions that increase efficiency. Workspaces can help drive productivity by:

- Providing 360-degree views of activities - No need to navigate to multiple lists.
- Answering specific questions such as:
 - Which customer invoices are past due now?
 - How many purchase orders have been received and are ready to be invoiced?
 - How many POS devices are activated?
- Providing insights – You can compare multiple sources of data and get a big picture view that might be difficult to achieve when only looking at lists in specific modules.
- Navigating by data – A workspace provides a concise view of the business data, which helps you search for results by spending less time on the filtering process.
- Providing direct access to tasks - Tasks can be performed directly from the workspace.

The screenshot depicts the user interface of a standard workspace:



Figure 1.1.12. The user interface of a standard workspace for managing customer credit and collections.

Analytical workspaces:

The Dynamics 365 suite of applications includes analytical workspaces. These workspaces include a set of reports that offer insights into standard business operations. These reports are like dashboards and differ from financial reports. You can design and embed the Microsoft Power BI reports in the analytical workspace. The reports include metrics that a wide range of users from any industry may find useful. You can change the reports if needed.

Users who have access to the web-friendly Power BI report design tools can customize their analytical reports. The free-form canvas designer in Power BI helps in designing relevant business insights. The designer provides better visibility of the business and helps to make the organization successful.

Mobile workspaces:

You can use mobile workspaces with several finance and operations mobile apps, including Timesheet, Expense, and Advanced Warehouse.

The mobile apps enable your organization to make business processes available on mobile devices. After your IT admin enables mobile workspaces for your organization, users can sign into the app, and immediately begin to run business processes from their mobile devices.

The mobile app includes the following features that can help increase productivity:

- Users can view, edit, and act on business data even if they have intermittent network connectivity or their mobile device is offline. When a device reestablishes a network connection, offline data operations are automatically synchronized.
- IT admins or developers can build and publish mobile workspaces that are tailored to an organization. The app uses your existing code assets. Therefore, you don't have to reimplement your validation procedures, business logic, or security configuration.
- IT admins or developers can easily design mobile workspaces by using the point-and-click workspace designer that is included with the web client.
- IT admins or developers can optimize the offline capabilities of workspaces by using the Business logic extensibility framework. Because data continues to be processed while a device is offline, your mobile scenarios remain rich and fluid, even if devices don't have constant network connectivity.

SUMMARY



- **Enterprise Resource Planning (ERP):**
ERP software streamlines various business operations, from finance to supply chain, by automating processes and providing real-time insights.
- **Dynamics 365 Overview:**
Dynamics 365 combines CRM and ERP capabilities in a cloud-based suite, offering tools for customer engagement, financial management, supply chain, commerce, and human resources.
- **Finance and Operations Apps:**
These apps offer real-time financial management, supply chain insights, enhanced customer engagement, improved HR management, and project-centric capabilities.
- **Dynamics 365 Business Central:**
Business Central is designed for small and mid-sized organizations, automating processes with lower user requirements and built-in CRM features.

- **Use Cases:**
Dynamics 365 apps are suitable for organizations facing growth challenges, disconnected systems, or high operating costs, offering scalability, insights, and cost-effectiveness.
- **User Interfaces:**
The apps have intuitive UI elements, including navigation, personalization options, action panes, and various filtering methods.
- **Workspaces:**
Workspaces provide consolidated views for specific tasks, including analytical workspaces with Power BI reports and mobile workspaces for on-the-go access.

MULTIPLE CHOICE QUESTIONS (MCQ) FOR PRACTICE

- 1 What does ERP stand for?
 - a) Enterprise Resource Process
 - b) Enterprise Resource Planning
 - c) Effective Resource Processing
 - d) Essential Resource Program
- 2 Which of the following is NOT a core function typically managed by ERP software?
 - a) Human Resources
 - b) Customer Relationship Management
 - c) Supply Chain Management
 - d) Social Media Marketing
- 3 Which Microsoft product offers customer engagement tools for marketing, sales, and customer service within the Dynamics 365 suite?
 - a) Dynamics 365 Business Central
 - b) Dynamics 365 Finance
 - c) Dynamics 365 for Customer Engagement
 - d) Dynamics 365 Supply Chain Management
- 4 What are the primary components of Dynamics 365 Finance and Operations apps?
 - a) Marketing and Sales
 - b) Financial Management and Human Resources
 - c) Supply Chain Management and Commerce
 - d) All of the above

- 5 Which type of organizations is Dynamics 365 Business Central primarily designed for?
- a) Large Enterprises
 - b) Small and Mid-sized Organizations
 - c) Non-profit Organizations
 - d) Educational Institutions
- 6 What is one common challenge that might prompt an organization to consider implementing ERP software?
- a) Lack of available office space
 - b) Excessive employee turnover
 - c) High operating costs
 - d) Frequent computer system updates
- 7 Which user interface element in Dynamics 365 provides access to frequently used pages for easy navigation?
- a) Navigation bar
 - b) Action Pane
 - c) Filter pane
 - d) Quick filter
- 8 In Dynamics 365, what is the purpose of the "Company picker" option in the navigation bar?
- a) It allows users to pick their favourite company.
 - b) It helps users select a legal entity for operations.
 - c) It enables users to change the company's name.
 - d) It offers a list of all companies using Dynamics 365.
- 9 What is the main advantage of using workspaces in Dynamics 365?
- a) They provide 3D visualization of data.
 - b) They offer real-time stock market updates.
 - c) They consolidate data, reports, and transactions to increase efficiency.
 - d) They allow users to play video games.
- 10 What types of reports are included in analytical workspaces in Dynamics 365?
- a) Financial reports
 - b) Employee performance reports
 - c) Power BI reports
 - d) Social media reports
- 11 What feature in Dynamics 365 allows users to record and play back business processes, create user manuals, and perform regression testing?
- a) Mobile workspaces
 - b) Task recorder
 - c) Analytical workspaces
 - d) Action Pane

- 12 Which deployment options are available for finance and operations apps in Dynamics 365?
- a) Cloud only
 - b) On-premises only
 - c) Both cloud and on-premises
 - d) Mobile app only
- 13 What does the "Filter pane" provide in Dynamics 365?
- a) Quick single-column filtering
 - b) An inline pane with multiple filter criteria
 - c) Advanced filter and sort capabilities
 - d) A list of recent pages
- 14 What does Dynamics 365 Business Central require as a minimum number of users for implementation?
- a) 5 users
 - b) 10 users
 - c) 20 users
 - d) 50 users
- 15 Which component of the Dynamics 365 User Options page allows users to configure language preferences and time zones?
- a) Visual
 - b) Preferences
 - c) Workflow
 - d) Account

Answers

- 1 *b. Enterprise Resource Planning*
- 2 *d. Social Media Marketing*
- 3 *c. Dynamics 365 for Customer Engagement*
- 4 *c. Supply Chain Management and Commerce*
- 5 *b. Small and Mid-sized Organizations*
- 6 *c. High operating costs*
- 7 *a. Navigation bar*
- 8 *b. It helps users select a legal entity for operations.*
- 9 *c. They consolidate data, reports, and transactions to increase efficiency.*
- 10 *c. Power BI reports*
- 11 *b. Task recorder*
- 12 *c. Both cloud and on-premises*
- 13 *b. An inline pane with multiple filter criteria*
- 14 *a. 5 users*
- 15 *b. Preferences*

**SELF-EXAMINATION QUESTIONS FOR PRACTICE:**

- 1 What is the primary purpose of Enterprise Resource Planning (ERP) software?
- 2 How does ERP software help organizations streamline their operations?
- 3 In Dynamics 365, what are the key components of the finance and operations apps?
- 4 What distinguishes Dynamics 365 Business Central from the finance and operations apps in terms of target users and functionality?
- 5 What are some common challenges that might prompt an organization to consider implementing finance and operations apps like Dynamics 365?
- 6 Describe the role of the navigation pane in the user interface of finance and operations apps.
- 7 How does Dynamics 365 address the need for mobile access to business processes?
- 8 What are the benefits of using workspaces in Dynamics 365, and how do they enhance productivity?

CHAPTER 2

DESCRIBE REPORTING AND INTEGRATION CAPABILITIES IN FINANCE AND OPERATIONS APPS



LEARNING OBJECTIVES

- Describe built-in reporting capabilities.
- Describe options for analyzing data.
- Describe options for working with data in Microsoft Office.
- Describe integration capabilities with Microsoft Power Platform.
- Describe business events.

2.1. INTRODUCTION

This module discusses the built-in reporting capabilities of finance and operations apps. It also discusses the integration capabilities of finance and operations apps with other Microsoft products, such as Excel, Outlook, Word, Microsoft Power Platform, and Microsoft Power Platform.

2.2. DESCRIBE ENTERPRISE RESOURCE PLANNING (ERP)

Finance and operations apps include pre-generated SQL Server Reporting Services (SSRS) reports. You can print reports to various locations such as your screen, a printer, a file, or to an email. You can use SSRS reports to create parameterized views that support drill-down navigation. You can also embed hyperlinks from a report to finance and operations apps pages.

You can schedule reports to run periodically by using a batch job. SSRS reports can help you create precise compliance documents for your local regulatory needs. In addition to the out-of-the-box reports, you can create custom reports that suit your organization's needs by using the SSRS tool and through X++ development.

Create SSRS reports:

To create a report, you need to use Microsoft Visual Studio and a finance and operations apps development environment. In Visual Studio, you first create a new report object. Then, you assign a data set to the report.

A data set defines the data that the report uses. In the data set parameters, you can select a data source for the data set and the data source type. The data source type explains how the system retrieves data from the data source.

The four data source types are:

- **Query** - Use an existing Application Object Tree (AOT) query. Using an existing query allows for faster data filtering in SQL to quickly generate reports and requires limited X++ code to develop. The only X++ code used is for the display methods in the tables.

- **Business logic** - Use a data source other than finance and operations apps. You can only use the business logic data source type with a single report because the name of the class used must match the name of the report.
- **Report data provider (RDP)** - Use when added logic is needed to run the report. This is usually the case when you use dynamic filters. An RDP class is an X++ class. You can apply advanced filter criteria to access and process data for the SSRS report. Report parameters, which are applied in the UI, can also be processed through the RDP class.
- **AX enum provider** - Use to filter a report view when the report parameter is an enumeration type. In these reports, the collection of enumeration values can be referenced by the report. AX enum provider allows you to add a dataset that binds to a specific enumeration, and it forces the report to display a specific enumeration value.

After you create a data set, you can set the report layout by selecting an auto design (for simple reports) or a precision design (for more customized reports). After you finish your report, you'll need to deploy it. After deployment, your report is ready to run in finance and operations apps.

Create and modify reports by using Power BI:

Power BI uses a series of software services, applications, and other connectors that work together to cohesively integrate unrelated sources of data to ensure they're both engaging and interactive. Power BI consists of several elements that all work together, including a Windows desktop application, an online software as a service (SaaS), and mobile apps. These elements let you easily connect to your data sources, visualize, and discover what is important, and then share that information with anyone you want.

You can use Power BI tools to interactively explore data by pivoting columns, changing the shape of charts, filtering data, and sharing reports. You can embed these reports within a workspace in finance and operations apps. Power BI is especially useful for creating dashboards and non-document reports or any report that doesn't require printing.

Ready-made Power BI reports are available in the shared asset library of Microsoft Dynamics Lifecycle Services, which can be downloaded and deployed in an environment. The following list provides examples of these reports:

- Actual vs. budget
- Cash overview
- Compensation and benefits
- Cost accounting analysis
- Credit and collections management
- Employee competencies and development
- Financial performance

- Fixed asset management
- Organizational training
- Practice manager
- Production performance
- Purchase spend analysis
- Recruiting
- Sales and profitability performance
- Vendor payments
- Warehouse performance
- Workforce metrics

The following Power BI content is available in the PowerBI.com marketplace, which you can deploy:

- Cost management
- Financial performance
- Retail channel performance

You may need to create your own Power BI reports by using Power BI Desktop. These reports can be uploaded to the Lifecycle Services project asset library. These uploaded reports can be deployed to the PowerBI.com account from the finance and operations apps or embedded in the workspace.

Create and modify reports by using Microsoft Excel:

You can use Excel for budget planning, financial reporting, and viewing and analyzing transactional data and other data such as customer and vendor data. Finance and operations apps can integrate with an Excel workbook, which can update, delete, and insert data within the finance and operations apps using the Excel Data Connector add-in. This add-in follows the REST-based integration protocol that connects the data entities of the finance and operations apps through the Open Data Protocol (OData) endpoints.

The Excel Data Connector uses transactional data configured in real-time where data is both uploaded and validated. The corresponding records appear in Dynamics 365 for immediate use. You must download the Microsoft Dynamics Office Add-in to use this feature.

Financial reporting:

Financial and business professionals rely on financial reporting for all aspects of their business. The finance and operations reporting capabilities enable these professionals to create, maintain, deploy, and view financial statements. These reports help you efficiently design many types of reports.

Financial reporting includes dimension support. Account segments or dimensions are immediately available with no extra tools or configuration steps required.

Many companies run a core set of financial reports at scheduled intervals to align with their business processes. Financial reporting allows regular report scheduling, such as daily, weekly, monthly, or annually.

2.3. DESCRIBE HOW TO USE POWER BI TO ANALYZE DATA

Dynamics 365 applications deliver interactive reports that integrate into application workspaces. Workspaces use rich infographics and visuals supported by Power BI to give you a highly visual and interactive experience. Using infographics in the overview page, you can get a quick glance of the state of the business.

Power BI:

Is a business analytics service that delivers insights to enable fast, informed decisions and helps you harness data and turn it into actionable insights.

Connects to hundreds of data sources using standard connectors and to unlimited data sources using custom connectors.

Simplifies how you derive insights from transactional and observational data, and helps you create a data culture where employees make decisions based on facts, not opinions.

Helps you collect data and display it as visually immersive, captivated, and interactive insights. The insights allow you to drill down and analyze financial and operational data.

An advantage of Power BI is the ability to include data from multiple sources including Excel workbooks and a collection of cloud-based and on-premises hybrid data warehouses. You can connect to your data sources, visualize what is important, and share the information with anyone you want.

The following illustration depicts a Power BI dashboard that includes data from Salesforce, Microsoft Access, Microsoft SharePoint, OneDrive, Excel, SQL databases, Microsoft Exchange, and Dynamics 365 business applications.



Figure 2.1. Power BI dashboard that has data from multiple sources.

Power BI for Office 365 cloud service works with model-driven apps in Dynamics 365 to provide a self-service analytics solution.

It refreshes the data displayed automatically. Your organization has a powerful new way to work with data with Power BI Desktop or Power Query for authoring reports, and with Power BI for sharing dashboards and refreshing data from model-driven apps in Dynamics 365.

Dashboards and reports in Power BI:

Power BI has dashboards and tiles to build visualizations using both browser-based, mobile, and desktop tools. When you need to see data analysis in the context of an opportunity record, you can consume Power BI tiles in other Dynamics 365 applications. You can also embed canvas apps on Power BI dashboards.

Two other elements extend the features of Power BI: Power BI Report Builder and Power BI Report Server. Report Builder is good for creating paginated reports to share in the Power BI Service. Report Server provides an on-premises report server where you can publish your Power BI reports after creating the reports in Power BI Desktop.

How you use Power BI depends on the role you hold in a project or on a team. You might primarily use the Power BI service to view reports and dashboards. A number-crunching, business-report-creating coworker might make extensive use of Power BI Desktop or Power BI Report Builder to create reports and then publish those reports to the Power BI service where you view them.

Analyze your financial data with embedded Power BI:

You can embed customized reports in the dashboard with the help of the Power BI desktop or Power BI services.

Custom visuals:

AppSource Power BI visuals:

Microsoft and community members contribute Power BI visuals for public benefit and publish them to AppSource, the place for apps, add-ins, and extensions for your Microsoft software. You can download these visuals and add them to your Power BI reports. Every product available in AppSource has been certified according to specific criteria.

Note:

By using Power BI visuals created with the Microsoft software development kit (SDK), you may be importing data from, or sending data to, third-party or other services located outside your Power BI tenant's geographic area, compliance boundary, or national cloud instance.

Power BI certified visuals are visuals in the AppSource that were additionally tested to confirm that the visual doesn't access external services or resources. When Power BI visuals from AppSource are imported, visuals may be updated automatically without any other notice.

Certified Power BI visuals:

Certified Power BI visualizations in AppSource meet certain specified code requirements that the Power BI team has tested and approved. The tests are designed to check that the visual doesn't access external services or resources.

Filter data with Power BI:

Data is the core of Power BI. As you explore reports, each visual draws its underlying data from sources that often have far more data than you need. Power BI offers several ways to filter and highlight reports. Knowing how to filter data is the key to finding the right information. The following illustration depicts the important features of the Power BI reporting tool.

Note:

Filtering only applies to reports, not to dashboards.

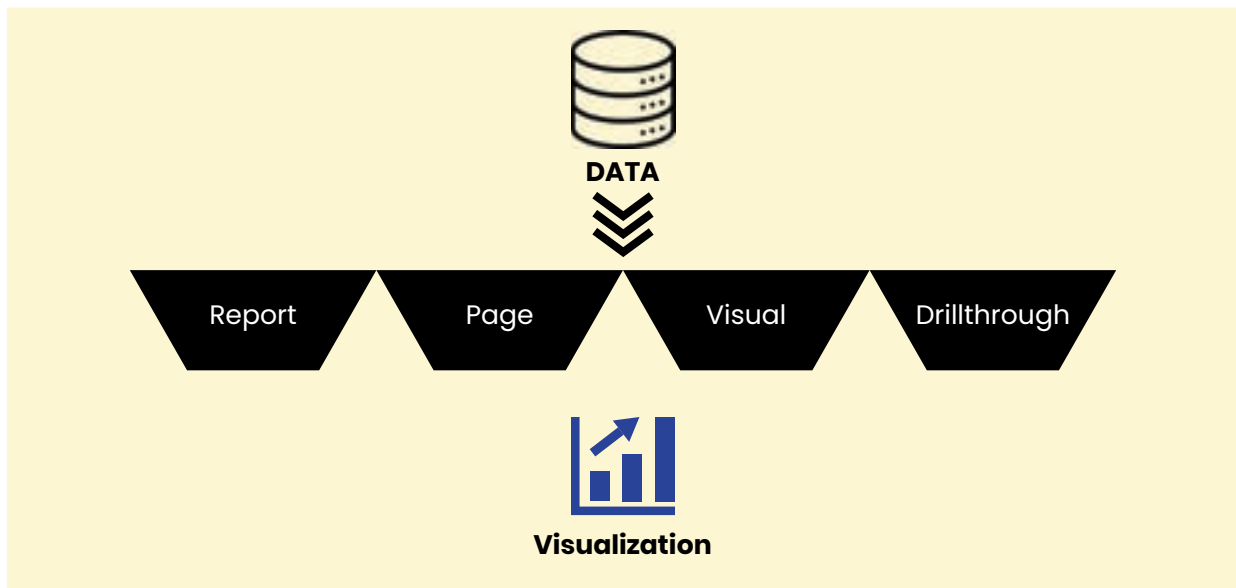


Figure 2.2. Filtering data with Power BI that illustrates that changing the different available filters will not affect the source data.

Note:

When you filter a visual, such as a bar chart, you're just changing the view of the data in that visual. You aren't changing the source data in any way.

Explore the Filters pane:

Another way to filter data is by opening and changing filters in the Filters pane. The Filters pane has filters that were added to the report by the report designer. As a consumer, you can interact with the filters and save your changes, but you can't add new filters.

The four types of filters are:

- **Report** – Applies to all pages in the report.
- **Page** – Applies to all the visuals on the current report page.
- **Visual** – Applies to a single visual on a report page. You only see visual level filters if you have selected a visual on the report canvas.
- **Drill through** – Allows you to explore successively more detailed views within a single visual.

Use buttons in Power BI:

Using buttons in Power BI lets you create reports that behave like apps, and thereby create an engaging environment so users can hover, select, and further interact with Power BI content. You can add buttons to reports in Power BI Desktop and in the Power BI service. When you share your reports in the Power BI service, the reports provide an app-like experience for your users.

To create a button in Power BI Desktop, on the Insert ribbon, select Buttons. A menu appears, where you can select the button you want from a collection of options, as depicted in the following screenshot:

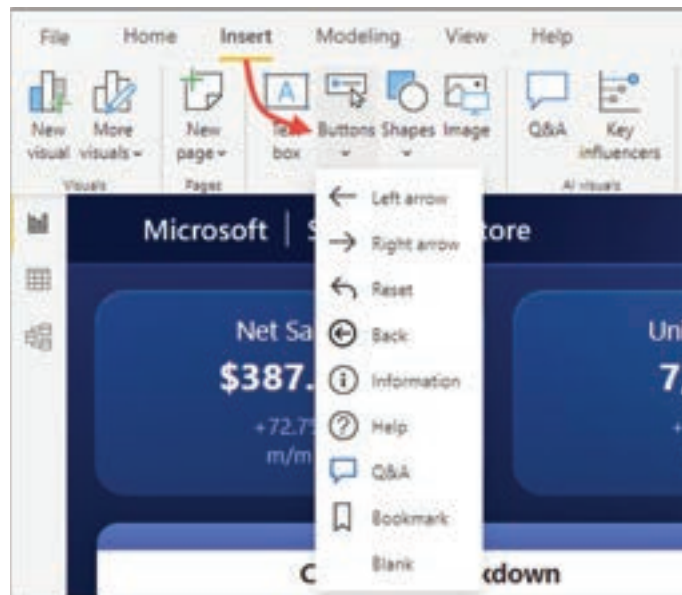


Figure 2.3. The callout of how to add a button control in Power BI desktop.

Transform data:

Sometimes, you may have too much data or the data might not be formatted correctly. Power BI Desktop includes the Power Query Editor tool, which can help you shape and transform data so that it's ready for your models and visualizations, as the following illustration depicts.

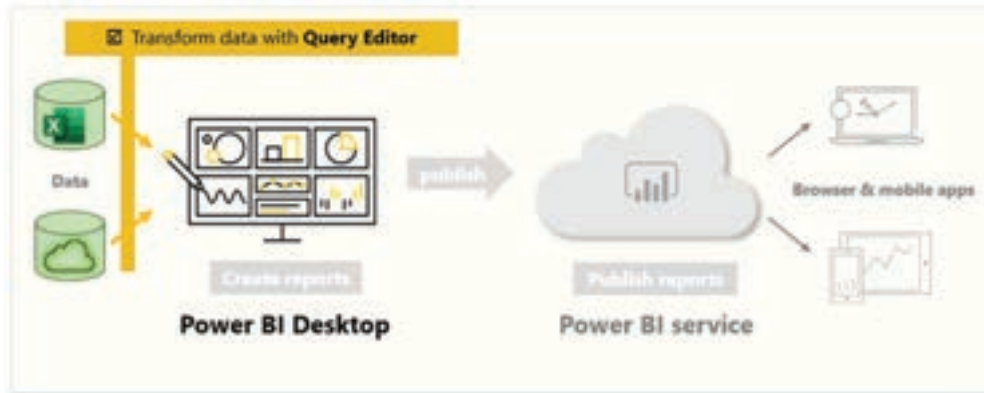


Figure 2.4. how to transform data with Query Editor.

2.4. DESCRIBE OPTIONS FOR MANIPULATING DATA FROM FINANCE AND OPERATIONS APPS WITHIN EXCEL

You can export data from finance and operations apps by using the Export to Excel feature, which is in the upper-right corner of most pages.

If you want to export data from the customer grid to Excel, you can select the option under Export to Excel, as depicted in the following screenshot. This process exports only those columns that are available in the grid. If you add a new column using the Personalize option, that column will also be exported to Excel.

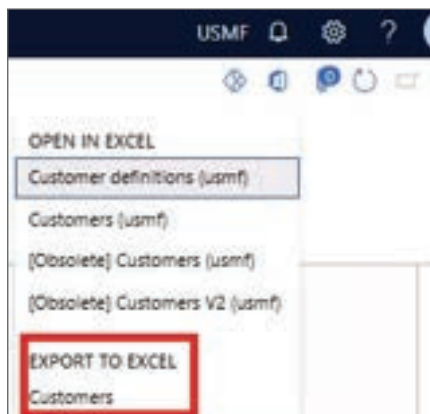


Figure 2.5. The Customers option selected under Export to Excel.

You can also trigger the Excel export by creating a custom button. To do so, you need to create a command button with the command Export to Microsoft Excel.

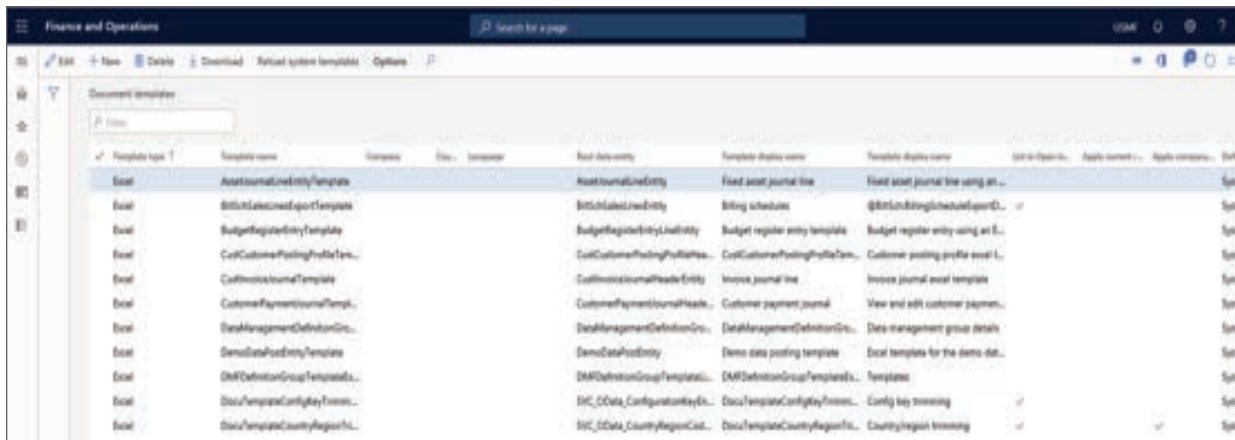
2.5. DESCRIBE MICROSOFT OFFICE 365 INTEGRATION CAPABILITIES

Microsoft Office:

Microsoft Office integration capabilities give you a productive environment that helps you get the job done by using Office products, such as Excel and Word. The key to this integration is the Microsoft Dynamics Office Add-in for Excel and Word.

The Microsoft Dynamics Office Add-in uses the existing Dynamics 365 OAuth security protocol. It retrieves the application security roles for the current user to supply consistent permissions. Users who don't have the proper permissions can't download sensitive data. The add-in app allows create, read, update, and delete operations on entities exposed as public.

Word and Excel are the most used business analysis applications. All Dynamics 365 apps have Microsoft Office integration capabilities. These templates span across all major system entities, such as projects, products, customers, and various journal entities. It's also possible to add other templates or edit the existing templates. You can find the document templates, depicted in the following screenshot, by navigating to Common > Common > Office integration > Document templates.



Template type	Template name	Entity	Doc. template	Doc. template	Template display name	Template display name	Doc. template	Apply context	Apply context
Excel	AssetJournalLineEntityTemplate	Asset	AssetJournalLineEntity	Fixed asset journal line	Fixed asset journal line using an...				
Excel	BillingScheduleExportTemplate	BillingSchedule	BillingScheduleEntity	Billing schedules	@BillingScheduleExportDoc...				
Excel	BudgetRegisterEntityTemplate	BudgetRegister	BudgetRegisterEntity	Budget register entity template	Budget register entity using an E...				
Excel	CostCustomerPostingProfileTemplate	CostCustomerPostingProfile	CostCustomerPostingProfileEntity	Cost customer posting profile tem...	Customer posting profile excel L...				
Excel	CustomerJournalTemplate	CustomerJournal	CustomerJournalHeaderEntity	Invoice journal line	Invoice journal excel template				
Excel	CustomerPaymentJournalTemp...	CustomerPaymentJournal	CustomerPaymentJournalHeader...	Customer payment journal	View and edit customer payment...				
Excel	DataManagementDefinitionGr...	DataManagementDefinitionGr...	DataManagementDefinitionGr...	Data management definition gr...	Data management group details				
Excel	DemoDataPostingTemplate	DemoDataPosting	DemoDataPostingEntity	Demo data posting template	Excel templates for the demo dat...				
Excel	DMPDefinitionGroupTemplate...	DMPDefinitionGroup	DMPDefinitionGroupTemplate...	DMP definition group template...	Templates				
Excel	DocTemplateConfigKeyInven...	DocTemplateConfigKeyInven...	DocTemplateConfigKeyInven...	Doc template config key inven...	Config key tracking				
Excel	DocTemplateCountryRegionL...	DocTemplateCountryRegionL...	DocTemplateCountryRegionL...	Doc template country region l...	Country/region tracking				

Figure 2.6. The Document templates used for the Office integration functionality.

Integrate with Excel:

Finance and operations apps use an out-of-the-box application called Excel Data Connector to view, update, and edit data within an Excel workbook. You need to download the Microsoft Dynamics Office Add-in, depicted in the following screenshot, to use this feature.



Figure 2.7. The Microsoft Dynamics Office add-in.

This feature is available at the upper-right corner of a page in the links under the Open in Excel menu, as depicted in the following screenshot:

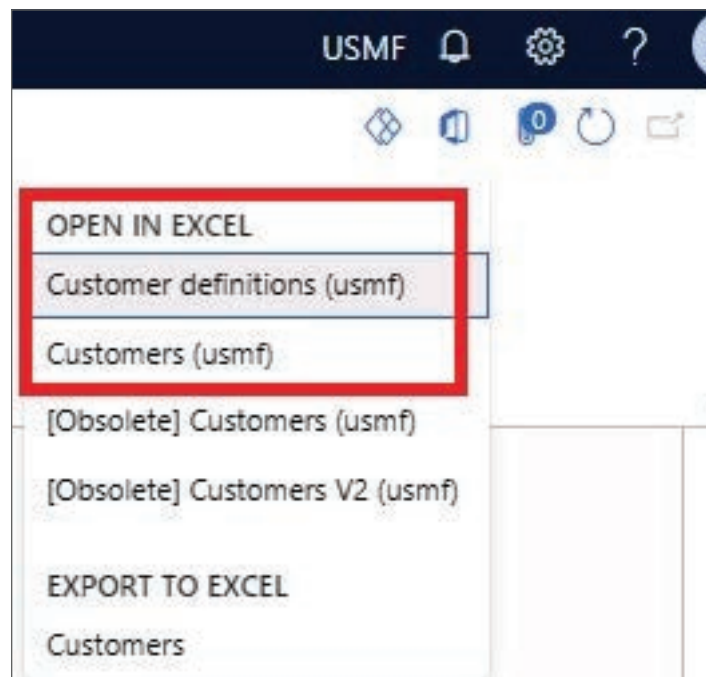


Figure 2.8. Highlights the Open in Excel option links.

Open in Excel lets you use the data entity that is related to the primary data source of the page. The columns that appear in your Excel workbook are defined in the Auto Report field group on the entity. You can also add or remove fields in Excel by using the Design button in the app. Additionally, you can filter the data by using the Filter button. The app also gives you the ability to change the data in Excel and publish the changes back to finance and operations apps.

Publish data by using the Excel add-in:

To ensure you publish valid data by using the Microsoft Dynamics Office Add-in, any updates pass through the existing data entity logic validation. This validation ensures data integrity and provides you with immediate feedback of relevant error messages if a data publish was unsuccessful.

What is a data entity?

A data entity is an object in a data model. You design data by breaking down things into the smallest parts that are useful for representing data relationships. For example, the vendor entity encompasses and combines over 17 different tables and data sources into a single vendor entity. During import or export events, entities use business logic to validate and transform the data being received or sent. Finance and operations apps also allow the creation of custom data entities. Each data entity has a property named Enable public API. If this property value is set to Yes, the data entity will automatically be exposed as an OData endpoint. Excel Data Connector can consume this OData endpoint and establish synchronous integration with finance and operations apps.

Open entity data in Excel:

To open the entity data, you can start from either Excel or the finance and operations apps. By opening entity data in Excel, you can quickly and easily view and edit the data by using the Microsoft Dynamics Office Add-in.

With the Microsoft Dynamics Office Add-in, you can:

- Open entity data in Excel when you start from the finance and operations apps.
- Open entity data in Excel when you start from Excel.
- View, edit, and update entity data in Excel.
- Add or remove columns. You can use the designer to adjust the columns that the system automatically adds to the worksheet.
- Copy configuration data from one environment to another using a workbook. However, you can't just change the connection URL because the data cache in the workbook continues to treat the data as existing data. Instead, you must use the Copy Environment Data functionality to publish the data to a new environment as new data.

The preceding features enable Excel to interact with finance and operations apps seamlessly through the OData endpoint.

Excel workbook designer:

Finance and operations apps have a simple-to-use interface to create Excel templates. It allows you to use data entities and the corresponding field definitions. You can use the Excel workbook designer page to design an editable custom export workbook that contains an entity and a set of fields.

Generated Open in Excel:

Generated Open in Excel options are automatically added to pages when the system finds data entities that have the same root data source as the page. The workbook that is generated will contain a single table data source where the data from that entity is loaded.

The Open in Excel experiences are listed on the Open in Microsoft Office menu. When an entity has the same root data source as a page, it's added as an option in the Open in Excel section of the Open in Microsoft Office menu. This is referred to as a generated option.

The Excel app has a design experience that lets users add and edit bindings to entity data sources and labels.

Microsoft Word:

You can use Export to Word experiences for lightweight reporting. These experiences are powered by prebuilt templates. Available Export to Word templates are listed on the Export to Word menu. The following screenshot depicts the menu available when the Open in Microsoft Office menu is selected from the upper-right corner of a page. The Export to Word option is available under this menu.

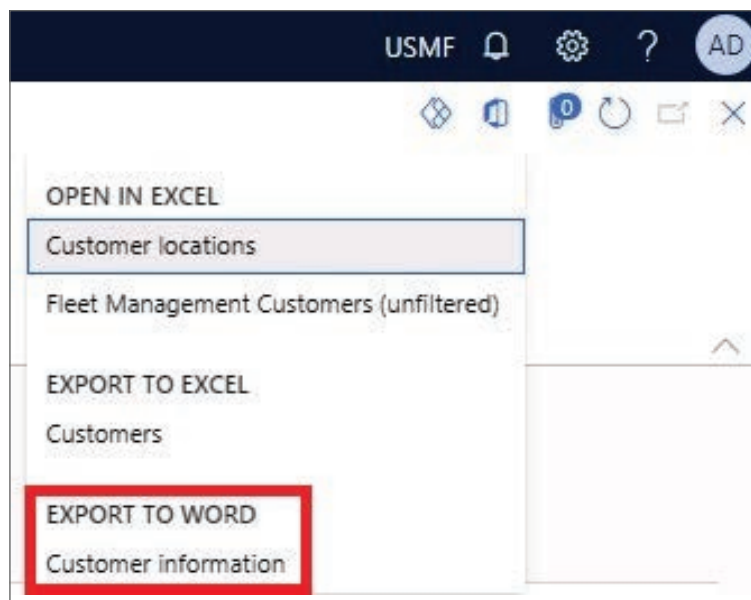


Figure 2.9. Open in the Microsoft Office menu with the Export to Word option highlighted.

To create a Word template,

- Navigate to Common > Common > Office integration > Excel workbook designer.
- Select the required entity and the fields you want to display in the Word template.
- Select the Create blank document button in the Action Pane once the field selection is complete.
- The system prompts you to download the Word template, which you need to design according to your reporting format.
- Navigate to Common > Common > Office integration > Document templates and upload the newly created Word template.

You should be able to see the Export to Word menu on the corresponding page.

The Export to Word option provides you with the report in the Word template with the data selected in the finance and operations apps.

Integrate with SharePoint:

SharePoint gives organizations a secure place to store, organize, share, and manage content, knowledge, and applications, which help the organization:

- Empower teamwork.
- Quickly find information.
- Seamlessly collaborate across the organization.

Information within SharePoint can be accessed from any device that has a web browser, such as Microsoft Edge, Chrome, or Firefox.

Note:

Before you can use SharePoint to store documents, it must be enabled by your system administrator.

Important:

This feature requires that you have a Microsoft 365 subscription or a subscription to an online service, such as SharePoint.

Document management using SharePoint:

Document management is a common framework in finance and operations apps that can be applicable for all the modules and pages. You can associate a file or an image with any record in the finance and operations apps by selecting the Attachments icon in the upper-left corner of your page, as depicted in the following screenshot.

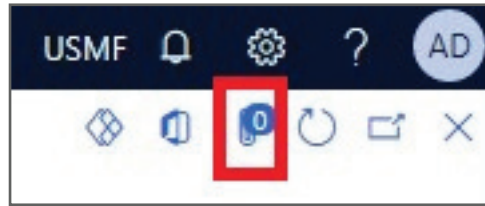


Figure 2.10. The options available in the upper-left corner of the page with the Attachments icon highlighted.

You can associate different types of documents with a record. These document types can be added under Organization administration > Document management > Document types.

As depicted in the following screenshot, selecting Attach file in the Class field allows you to select SharePoint in the Location field. In the SharePoint Address field, you can provide the SharePoint location where files will be stored.



Figure 2.11. The Document types page with SharePoint enabled.

Email integration:

The behavior of the email subsystem is influenced by a combination of administrator configuration, user configuration, and user choices. Both administrators and users set the behavior of the email subsystem.

Behaviors set by administrators:

- 1 Configuration tab
 - o Batch email provider - Specifies which email provider the system uses to send emails that are generated by processes in a batch or non-interactive manner. The Exchange provider uses the account associated with the batch process.
 - o Attachment size limit - Specifies the maximum size of a single email that can be sent by using the email subsystem.
- 2 SMTP settings tab
 - o Outgoing mail server - The host name of the desired SMTP server.
 - o SMTP port number - Typically, the port number should be set to 587 for secure transport.

- o Username and password – Specify, as needed, to send the email from the proper mail account. All users must have SMTP account Send As and Send On Behalf Of permissions to send Simple Mail Transfer Protocol (SMTP) mail.

You can configure Send As permissions in the Microsoft 365 admin center (admin.microsoft.com). Navigate to Users, select User under Active users. Then, select Send email from this mailbox under Edit mailbox permissions.

- o Specify whether SSL is needed – Determines whether secure transport is used. SSL is typically needed in all situations except for internal testing or troubleshooting scenarios.

Email distributor batch process:

Email that is sent directly from the server, without user interaction, is sent by the Email distributor batch process via SMTP. That batch process must be started to process the email queue.

If the Exchange provider is used, then the user account associated with the batch process (usually admin) will be sender.

User email:

The default send from address for each user is pulled from the Email field on the Users page. (Navigate to Users and then Users again in System administration.) Administrators can override this send from default if needed by using the Sender email field on the Options page.

Behaviors set by users:

Email provider selection section on the Options page

- **Email provider ID** – Allows the user to select the email provider that should be used when sending an email. Selecting an option here's the equivalent of selecting Do not ask again in the How would you like to send email dialog box. Selecting the blank option Prompt for which email provider to use causes the How would you like to send email dialog box to display when an email is going to be sent.
- **Sender email** – Allows the administrator to provide an email address override for the user in the From field of the email. By default, the email alias that is associated with the user account is used as the From field in new emails, but this user option email address overrides that. When a user sends email via SMTP, the user needs to have appropriate Send As and Send On Behalf Of permissions configured in Exchange or on the SMTP server.

How would you like to send email dialog box (optional)?

When you send an email, the How would you like to send email dialog box opens with a list of available options for sending email.

- Use an email app, such as Outlook – Provides the user with a generated email (.eml) file.
- Use Exchange email server – Uses the Exchange Online server associated with the tenant. On-premises Exchange servers are currently not supported for the Exchange mail provider.
- Use the system email client – Opens the Send email composition dialog box and then sends the resulting email via SMTP.
- Do not ask again – If this field isn't selected, the next time an email is sent the most recently selected option will be used and the dialog box won't open.

Send email dialog box (optional):

The Send email dialog box is opened to allow the user to edit the contents of the email that will be sent. The following fields may be prepopulated in this window.

- From – Populated from the Email field on the Options page.
- To, Cc, Bcc, Subject, and Body – Populated with values specified by the process that initiated the sending of the email. Users can edit these fields as needed.
- Attachments list – May be populated with attachments specified by the process that initiated the sending of the email. Users can edit this list as needed.

2.6. DESCRIBE OPTIONS FOR INTEGRATING FINANCE AND OPERATIONS APPS WITH MICROSOFT POWER PLATFORM

The current versions of finance and operations apps are hosted on Azure, which helps increase the integration scope of these products. These apps can connect to several other products hosted in Azure. They can also connect to the on-premises applications by using a gateway. We now explore the finance and operations apps integration capabilities with Microsoft Power Platform.

Microsoft Power Platform:

Microsoft Power Platform provides a suite of capabilities for finance and operations apps. Features like dual-write and virtual entity can establish direct integration between Microsoft Dataverse and data entities of finance and operations apps.

Microsoft Power Platform is made up of tools like canvas apps, Power Automate, and Power BI. All these tools can be individually integrated with finance and operations apps.

Integration with Dataverse:

Dataverse is the default data storage option for Microsoft Power Platform, where you can securely store your business data in tabular format, maintaining key and table relationships. Finance and operations apps, such as Finance, Supply Chain Management, and Commerce, store data in Azure SQL. However, we can integrate finance and operations apps with Dataverse by using the data entity framework. Several technologies are involved to achieve this integration.

Dual-write:

Dual-write is a standard integration platform that provides near-real-time interaction between Dataverse and finance and operations apps. It provides a tightly coupled, bidirectional integration capability, delivering a user-friendly experience across the apps.

Dual-write infrastructure follows a no-code/low-code principle, minimizing engineering effort to map standard or custom tables between apps. Dual-write supports both online and offline modes of operations. The following illustration depicts the dual-write capabilities.

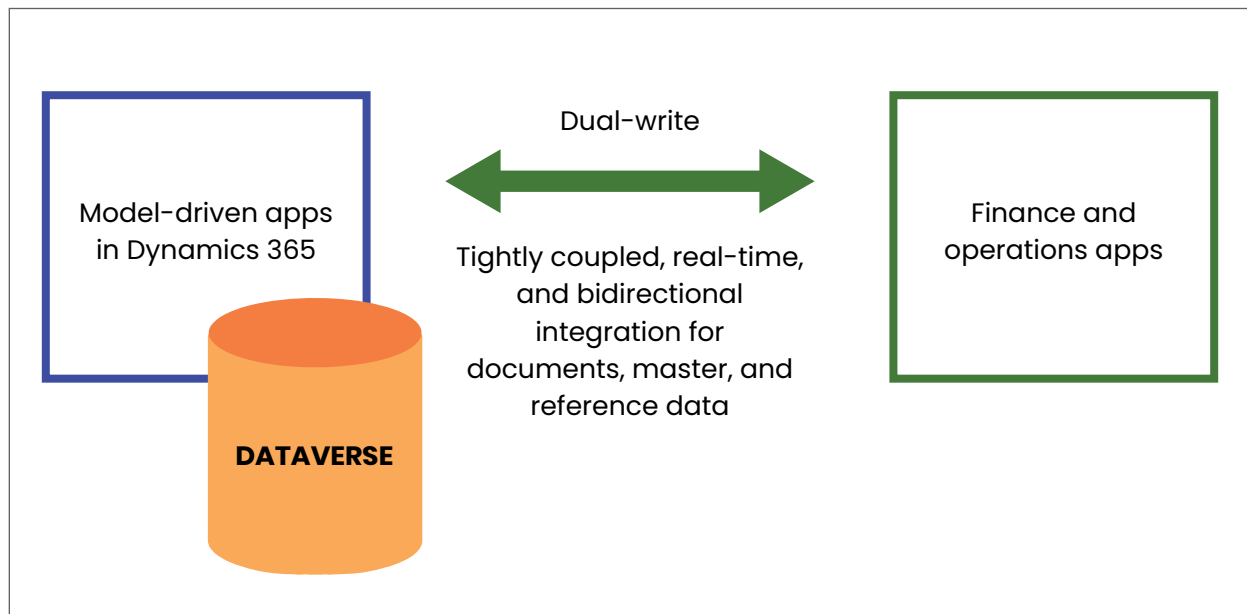


Figure 2.12. How dual-write supports both online and offline modes of operation.

Virtual entity:

Virtual entities enable the integration of data residing in external systems by seamlessly representing that data as tables in Dataverse, without replication of data and often without custom coding. The data sources of the finance and operations apps can also be used as a virtual data source in Dataverse. You can enable the full create, read, update, and delete (CRUD) operations from Dataverse on the finance and operations apps virtual entities.

All OData entities in finance and operations apps are available as virtual entities in Dataverse and therefore also in Microsoft Power Platform. You can create a model-driven app using the virtual entities and perform the CRUD operations directly on the finance and operations data source from your model-driven app. The following illustration depicts the integration capabilities of using virtual entities.

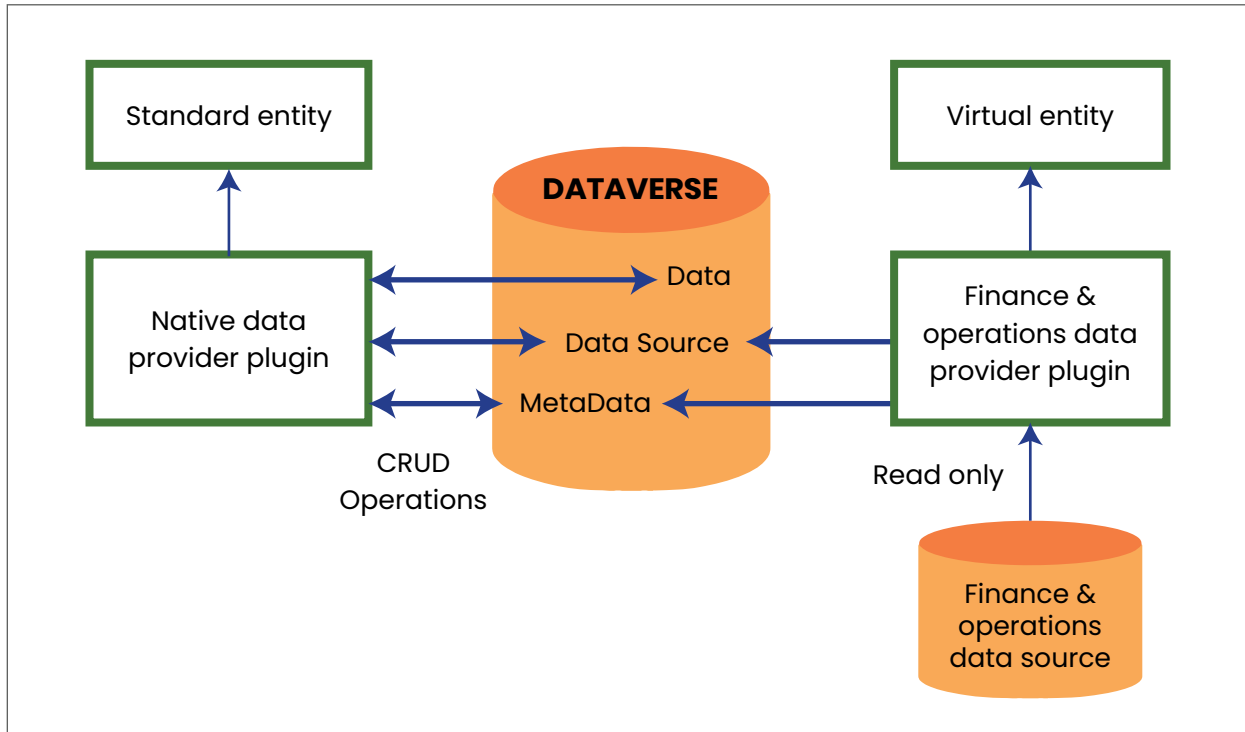


Figure 2.13. How to execute the CRUD operation directly on the finance and operations data source from your model-driven app.

Integration with a Power Apps canvas app:

A Power Apps canvas app is a no-code app development platform in Microsoft Power Platform. It has the capability to connect to various data sources using the built-in or custom connectors. To build a canvas app, you need to drag the control elements and drop them onto the canvas, designed for a mobile device or tablet. You can achieve canvas app integration with finance and operations apps in the following two ways.

Embed a canvas app in finance and operations apps:

Navigate to a page in the finance and operations apps. The upper-right corner of the page has an option to connect to a Power Apps canvas app, as depicted in the screenshot:

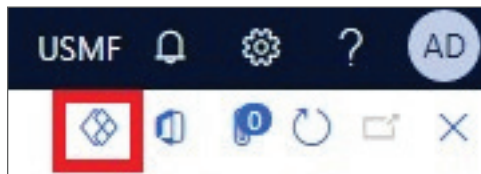


Figure 2.14. The options available in the upper-right corner of the page with the icon to embed a Microsoft Power Apps canvas app highlighted.

You can select the Add an app button under the Power Apps icon to embed the canvas app into the finance and operations apps. The following dialog box appears in the right panel of the finance and operations apps.

Figure 2.15. The dialog box to provide the Power Apps canvas app details.

You need to enter the following information:

- Name: The name of the canvas app.
- App ID: The app ID of the canvas app. You can select your canvas app to embed and select the Details button in the Action Pane of the Power Apps maker portal to get the app ID of the canvas app.
- Input context for the app: You can select a column from the data source of the current page of the finance and operations app. This field value is passed as a parameter to the canvas app for further data processing.
- Application size: You can select Thin or Wide. The canvas app is embedded in the finance and operations apps user interface based on your selection.

You can perform CRUD operations in the canvas app, which is embedded in the finance and operations app. The record in the canvas app will be related to the record selected in the finance and operations apps.

Connect a finance and operations data source from a canvas app:

You can directly connect to a finance and operations data source from the Power Apps canvas app by using the Fin & Ops Apps (Dynamics 365) data connector as depicted in the screenshot:

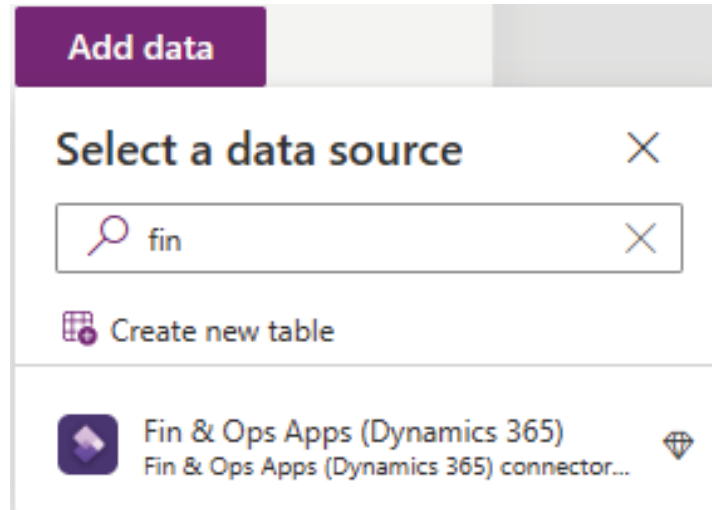


Figure 2.16. The Fin and Ops Apps (Dynamics 365) connector to connect to the finance and operations data source.

This enables you to create a mobile app using a Power Apps canvas app that has finance and operations as the back-end data source. This mobile app can perform all CRUD operations directly in the finance and operations apps database. All OData entities in finance and operations apps are available as data sources for the canvas app. For custom tables, you can create custom OData endpoints, which can be connected to the canvas app for the mobile app development activity.

Microsoft Power Apps integration:

This integration is possible even if the back-end data source of the canvas app is any third-party application.

Integration with Power Automate:

Power Automate is an online workflow service that automates actions across the most common apps and services. It can connect to multiple applications using data connectors and passes parameters across apps and services. Power Automate has a connector for finance and operations apps, which helps connect all the OData entities in finance and operations apps and performs CRUD operations on those entities. Power Automate primarily has two components: trigger and actions.

Trigger:

The Fin & Ops Apps (Dynamics 365) connector for Power Automate has a single trigger that can be initiated from a business event, as depicted in the screenshot:

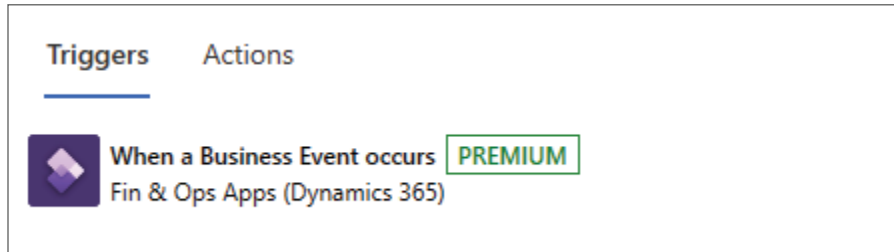


Figure 2.17. The Power Automate trigger that can be initiated from a business event in the Fin and Ops Apps (Dynamics 365 connector).

Business events provide a mechanism that lets external systems receive notifications from finance and operations apps. In this way, the systems can perform business actions in response to business events.

Business events occur when a business process is run. During a business process, users who participate in it perform business actions to complete the tasks that make up the business process.

Action:

The Fin & Ops Apps (Dynamics 365) connector for Power Automate supports several actions to perform on finance and operations apps, as depicted in the screenshot:

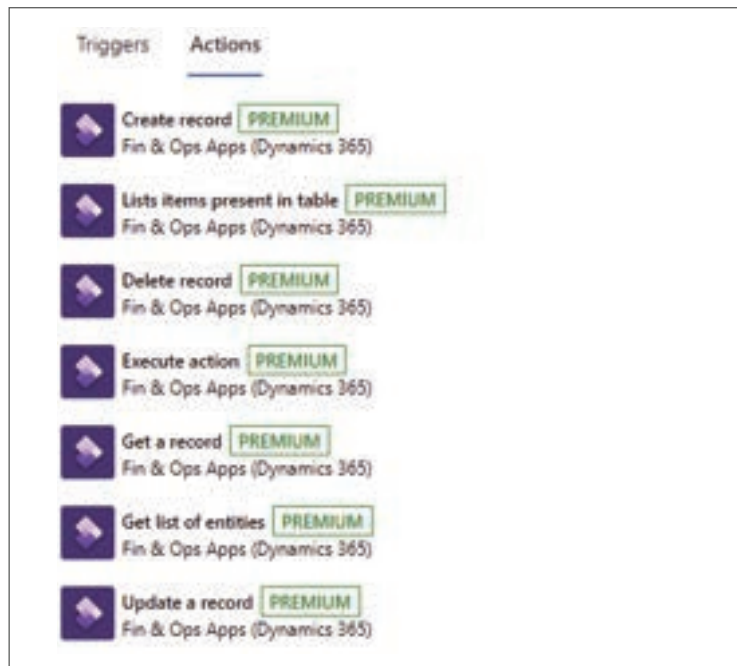


Figure 2.18. The Fin and Ops Apps (Dynamics 365) connector for Power Automate that shows actions to be performed on the finance and operations apps.

You can create, update, and delete data in your finance and operations apps. You can also read records and perform custom actions on the records based on business requirements. You can also connect other data connectors, such as Dataverse, SharePoint, and Outlook, with the Fin & Ops Apps (Dynamics 365) connector. This enables you to pass on data between the finance and operations apps and the other connected apps.

Following are the lists of actions that can be performed from Power Automate in finance and operations apps.

- **Create Record:** This action can be used to create a new record in finance and operations apps. Once the data entity is selected, all the columns of the selected entity are available to be updated in the connector. The values to be inserted in each column can be updated in Power Automate. Once Power Automate executes, a new record is created in the finance and operations underlying tables of the data entity.
- **List items present in the table:** This action can be used to get the list of records from an entity. This action supports cross-company reading of data.
- **Delete record:** This action can be used to delete an existing data record for a data entity. The usage is the same as the Get a Record action.
- **Execute action:** This action can be used to invoke methods on a data entity to perform a business action.
- **Get a record:** This action can be used to fetch a record for a specific data entity from the target instance.
- **Get the list of entities:** This action can be used to get the list of entities for further use in the app that is being developed.
- **Update a record:** This action can be used to update an existing data record for a data entity. The usage is the same as for the create a record action in this list.

2.7. EXPLORE BUSINESS EVENTS INTEGRATION CAPABILITIES

Using a business event, you can send a notification to an external system from finance and operations apps. Based on the notification, business actions can be performed in the external application.

Business events can be triggered from finance and operations apps based on an activity, including triggering a workflow, confirming a purchase order, posting a journal, and creating, updating, or deleting an operation on a table. Several standard business events are already available, as depicted in the following screenshot. You can find them under System administration > Setup.

The screenshot shows the 'Business events' page in Microsoft Dynamics 365. The 'Endpoints' tab is active, and the 'Purchase order confirmed' event is selected. The interface includes a navigation bar with 'Business event catalog', 'Data event catalog', 'Endpoints', 'Active business events', 'Inactive business events', 'Errors', and 'Security'. A '+ Activate' button is visible. The main table lists various business events with columns for Category, Business event ID, and Name. The 'Purchase order confirmed' event is highlighted, and its details are shown on the right, including a description and a 'Download schema' button.

Category	Business event ID	Name
Accounts receivable	CollectionStatusUpdated...	Collection status of a transaction chang...
Accounts receivable	CustFreeTextInvoicePoste...	Free text invoice posted
Accounts receivable	CustInterestNotePostedE...	Interest note posted
Accounts receivable	CustomerPaymentPosted...	Payment posted
Accounts receivable	CustWriteOffPostedBusin...	Transaction is written off
Purchase orders	BusinessEventsTestableOr...	Testable Order Post Event
Purchase orders	BusinessEventsTestEvent...	Testable Event with a long contract
Purchase orders	PurchaseOrderConfirmed...	Purchase order confirmed
Purchase orders	PurchaseOrderReceivedE...	Purchase order received
Accounts payable	VendorInvoiceApproval...	Invoice approval journal posted
Accounts payable	VendorInvoiceJournalPost...	Invoice journal posted
Accounts payable	VendorInvoiceMatchedBu...	Vendor invoice matched
Accounts payable	VendorInvoicePostedBus...	Vendor invoice posted
Accounts payable	VendorInvoiceRegisterPos...	Invoice register journal posted
Accounts payable	VendorPaymentPostedBu...	Vendor payment posted
Human resources	LeaveRequestWorkflowCo...	Leave request workflow completed
Human resources	LeaveRequestWorkItems...	This business event is raised whenever a...
Expense management	BusinessEventsApplicatio...	@ApplicationFoundationUnitTests Testa...

Purchase order confirmed

Purchase orders

This business event is triggered when a purchase order is confirmed by a vendor. One of the following actions triggers the event: the user manually confirms a purchase order in the user interface for purchase orders, when the purchase order confirmation is executed in a batch, or when the confirmation is executed programmatically in intercompany scenarios. In scenarios where vendor collaboration is used, and the vendor collaboration policy is set to auto-confirm a purchase order, the trigger occurs when the "Accept" button is clicked on the Purchase order confirmation page in the Vendor collaboration portal.

Fields passed to event

Download schema

Field name	Field label
LegalEntity	Legal entity
PurchaseJournal	Purchase journal
PurchaseType	Purchase type
PurchaseOrderDate	Purchase order date
PurchaseOrderNumber	Purchase order numit
TransactionCurrencyCode	Transaction currency

Figure 2.19. Business events.

You can create custom business events through code development, and they appear in the list depicted in the preceding screenshot. Each business event provides a JSON schema that you can download by selecting the Download schema option.

An external application can consume this JSON file and take appropriate actions based on business requirements. There are several endpoints that are exposed from the business event for external consumption. The following are the endpoints currently supported by finance and operations apps:

- Azure Service Bus Queue
- Azure Service Bus Topic
- Azure Event Grid
- Azure Event Hubs
- HTTPS
- Azure Blob Storage

To activate these endpoints, select the Endpoints tab and then select the New button. It provides you with the list of endpoints, from which you can select the one that is applicable for your requirements. Different endpoints have different configuration criteria. Once the business event is triggered in a finance and operations app, such as purchase order confirmation or journal posting, the JSON file is generated and sent through the selected endpoints.

Power Automate is another widely used endpoint for business events. To activate a Power Automate endpoint, you need to open the Power Apps maker portal and create a Power Automate trigger using the Fin & Ops Apps (Dynamics 365) data connector. Once you select the only available trigger. When a Business Event occurs, you are asked to enter the information depicted in the screenshot:

Figure 2.20. When a Business Event occurs trigger.

- Instance: Enter the finance and operations app environment URL.
- Category: Select the business event category.
- Business event: Select the business event that you want Power Automate to consume.
- Legal entity: Select the legal entity for which the trigger is applicable.

The trigger consumes the JSON file received from the finance and operations app. The JSON file is then parsed and processed for further business actions.

The Business event page has a Security tab where you can define role-based security for the business events.

Business events in Dynamics 365 finance and operations apps:

It's also possible to configure other endpoints to consume the JSON file triggered from the finance and operations apps.



SUMMARY

- 1 Reporting Options:
 - o Built-in SQL Server Reporting Services (SSRS) reports in finance and operations apps.
 - o Creation of custom SSRS reports using different data source types.
 - o The process of creating SSRS reports in Microsoft Visual Studio.
 - o Four data source types: Query, Business logic, Report data provider (RDP), and AX enum provider.
- 2 Using Power BI for Data Analysis:
 - o Power BI's role in data analysis, visualization, and report creation.
 - o Availability of ready-made Power BI reports in Microsoft Dynamics Lifecycle Services.
 - o Features of Power BI, including data source connectivity, interactive exploration, and report sharing.
 - o Embedding Power BI reports within finance and operations apps.
- 3 Manipulating Data in Excel:
 - o Exporting data from finance and operations apps to Excel using the Export to Excel feature.
 - o Triggering Excel exports through custom buttons.
 - o Utilizing Excel Data Connector for real-time data integration.
- 4 Microsoft Office 365 Integration:
 - o Integration with Microsoft Office products, specifically Excel and Word.
 - o The significance of the Microsoft Dynamics Office Add-in for Excel and Word integration.
 - o Excel Data Connector for data interaction.
 - o Document management via SharePoint and email integration features.
 - o Explanation of various settings and behaviors related to email integration for users and administrators.
- 5 Finance and operations apps on Azure integrate with various products, including on-premises apps.
- 6 Microsoft Power Platform offers integration tools like dual-write and virtual entity for connecting to finance and operations data.
- 7 Power Apps canvas apps can be embedded in or connect to finance and operations apps.

- 8 Power Automate automates actions across apps and services, including finance and operations.
- 9 Business events trigger notifications to external systems, with options like Power Automate for integration.
- 10 Custom business events can be created for specific actions in external apps based on JSON schemas.

MULTIPLE CHOICE QUESTIONS (MCQ) FOR PRACTICE

- 1 What are the primary learning objectives of the module on reporting and integration capabilities in finance and operations apps?
 - a) Developing custom reports and dashboards
 - b) Understanding Microsoft Word integration
 - c) Describing built-in reporting capabilities
 - d) Learning advanced Excel functions
- 2 Which tool is used to create custom reports in finance and operations apps?
 - a) Microsoft Excel
 - b) Microsoft Visual Studio
 - c) Microsoft Power BI
 - d) Microsoft Word
- 3 What is the purpose of a data set in creating SSRS reports?
 - a) To define the layout of the report
 - b) To select a data source for the report
 - c) To specify the report's audience
 - d) To schedule report execution
- 4 Which data source type allows for faster data filtering in SQL and requires limited X++ code to develop SSRS reports?
 - a) Business logic
 - b) Query
 - c) Report data provider (RDP)
 - d) AX enum provider

- 5 What is Power BI primarily used for in finance and operations apps?
- a) Creating compliance documents
 - b) Developing custom reports
 - c) Interactively exploring and visualizing data
 - d) Printing financial statements
- 6 Where can you find ready-made Power BI reports for finance and operations apps?
- a) In Microsoft Dynamics Lifecycle Services
 - b) In Microsoft Word templates
 - c) In Microsoft Excel workbooks
 - d) In Microsoft SharePoint
- 7 How can you embed Power BI reports within a workspace in finance and operations apps?
- a) By using Microsoft Word
 - b) By downloading a Power BI add-in
 - c) By using Power BI tools to create custom visuals
 - d) By using Power BI Desktop or Power BI services
- 8 What is the primary purpose of the Excel Data Connector add-in in finance and operations apps?
- a) To create financial statements
 - b) To automate data entry
 - c) To connect Excel workbooks to data entities
 - d) To create custom visuals in Excel
- 9 What types of filters can be applied in Power BI to refine data visualization?
- a) Page and visual filters
 - b) Page and report filters
 - c) Visual and drill-through filters
 - d) Report and drill-through filters
- 10 How can you export data from finance and operations apps to Excel?
- a) By using the Export to Excel feature in the upper-right corner of most pages
 - b) By creating a custom button with the command "ExportToMicrosoftExcel"
 - c) By using the Power BI Desktop application
 - d) By copying and pasting data directly from the app to Excel
- 11 What is the key to integrating Microsoft Office products like Excel and Word with Dynamics 365?
- a) Microsoft Dynamics Office Suite
 - b) Microsoft Dynamics Office Integration Tool
 - c) Microsoft Dynamics Office Add-in
 - d) Microsoft Dynamics 365 Integration Hub

- 12 How does the Microsoft Dynamics Office Add-in ensure data security in Dynamics 365?
- a) It encrypts all data before integration.
 - b) It restricts access to sensitive data for users with improper permissions.
 - c) It uses a separate security protocol.
 - d) It doesn't have data security features.
- 13 What are the most commonly used business analysis applications integrated with Dynamics 365?
- a) PowerPoint and Outlook
 - b) Excel and Word
 - c) SharePoint and Teams
 - d) OneNote and Access
- 14 Where can you find document templates for Office integration in Dynamics 365?
- a) Under the Excel Data Connector menu
 - b) In the Office 365 Admin Center
 - c) By navigating to Common > Common > Office integration > Document templates
 - d) In the Microsoft Office Online Store
- 15 Which feature allows you to interact with finance and operations apps seamlessly through the OData endpoint?
- a) Excel Data Connector
 - b) SharePoint Integration
 - c) Data Entity Validation
 - d) Document Templates

Answers

- 1 *Describing built-in reporting capabilities*
- 2 *Microsoft Visual Studio*
- 3 *To select a data source for the report*
- 4 *Query*
- 5 *Interactively exploring and visualizing data*
- 6 *In Microsoft Dynamics Lifecycle Services*
- 7 *By using Power BI Desktop or Power BI services*
- 8 *To connect Excel workbooks to data entities*
- 9 *Page and visual filters*
- 10 *By creating a custom button with the command "ExportToMicrosoftExcel"*
- 11 *Microsoft Dynamics Office Add-in*
- 12 *It restricts access to sensitive data for users with improper permissions.*
- 13 *Excel and Word*
- 14 *By navigating to Common > Common > Office integration > Document templates*
- 15 *Excel Data Connector*

**SELF-EXAMINATION QUESTIONS FOR PRACTICE:**

- 1 What are the key learning objectives of the module on reporting and integration capabilities in finance and operations apps?
- 2 How can SSRS reports be used in finance and operations apps, and what options are available for creating custom reports?
- 3 Describe the role of Power BI in analyzing data within finance and operations apps. How does it integrate with other Microsoft products?
- 4 Explain the various ways to export data from finance and operations apps to Excel and the options for customizing these exports.
- 5 What are Microsoft Office integration capabilities, and which key add-in enables this integration with Dynamics 365?
- 6 Which business analysis applications commonly integrate with Dynamics 365, and what types of templates are available for integration?
- 7 What are the key features of the Excel add-in for publishing data back to finance and operations apps?
- 8 What is a data entity in the context of finance and operations apps, and how does it relate to Excel Data Connector integration?
- 9 How can you open entity data in Excel, and what operations can you perform using the Microsoft Dynamics Office Add-in?
- 10 What is the purpose of the Excel workbook designer in finance and operations apps?
- 11 How does SharePoint integration benefit organizations in storing and managing content and documents, and what are the prerequisites for using SharePoint integration in Dynamics 365?

CHAPTER 3

LEARN THE FUNDAMENTALS OF MICROSOFT DYNAMICS 365 FINANCE



LEARNING OBJECTIVES

- Describe Finance capabilities, features, and use cases.
- Describe organization and legal entities.
- Describe number sequence functionality.
- Describe Finance tax capabilities.
- Describe cost accounting concepts.

3. DESCRIBE DYNAMICS 365 FINANCE CORE CAPABILITIES

3.1 INTRODUCTION

To get the most out of Finance, you first need to become familiar with its core capabilities and features. We cover units including general ledger and cash and bank management and how to use Finance for receiving money from customers and paying vendors.

We also explore how to create legal entities and prepare them for financial management.

Another topic we explore is that businesses must collect and pay taxes to various tax authorities. Different countries or regions have different rules and rates. Finance offers a comprehensive Tax module to help handle regional tax reporting requirements.

Finally, we discuss how to use cost types to track costs and journals to track transactions.

3.2. DESCRIBE FINANCE CAPABILITIES AND FEATURES

Finance is designed for the multi-company, multi-currency business of an organization and monitors the performance of a company on a real-time basis. Finance forecasts future results and makes data-driven decisions to boost the growth of the organization, regardless of its size and the industry in which it operates. The following illustration highlights some of the capabilities of Finance.

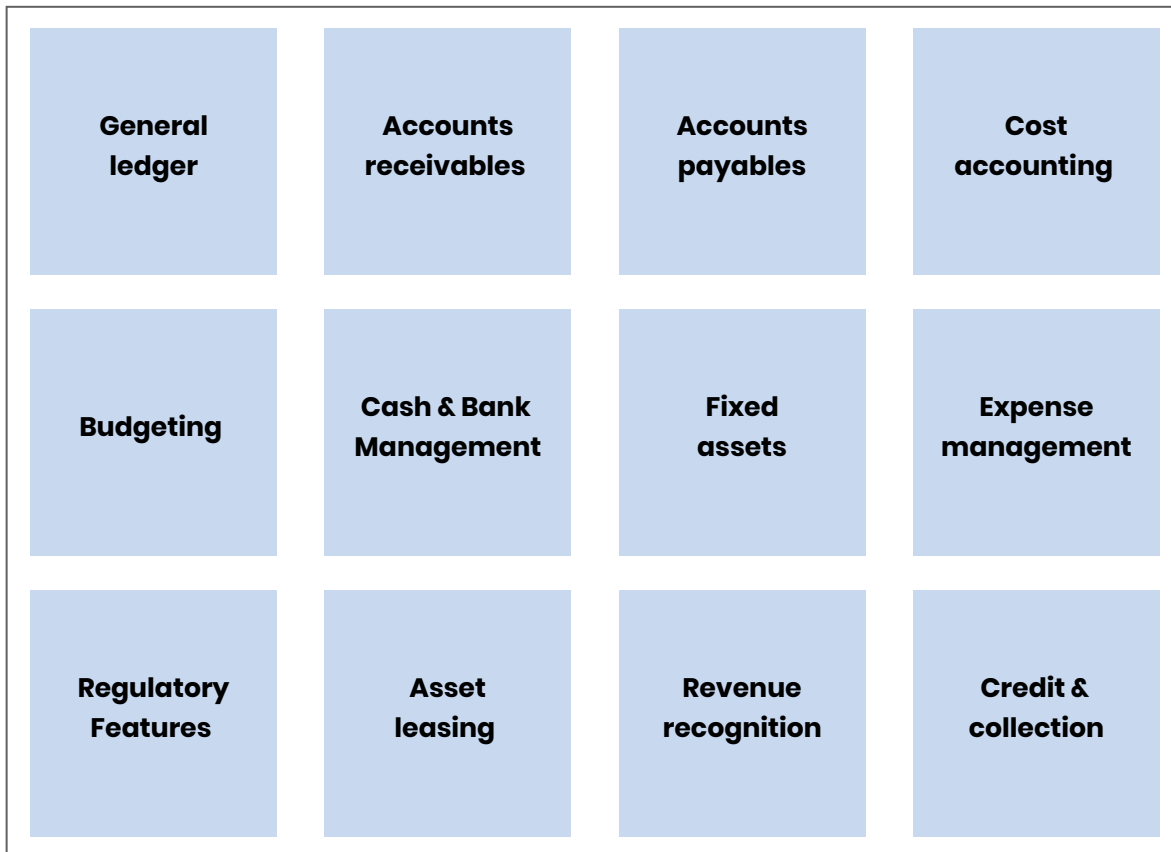


Figure 3.1.Finance capabilities and features.

General ledger:

The general ledger module is used to define and manage a legal entity's financial records. The general ledger is a register of debit and credit entries. These entries are classified using the accounts that are listed in a chart of accounts.

Use case: An organization is implementing Finance to digitize their finance and accounting system. General ledger is the first module to be designed. You need to configure the fiscal year followed by the chart of accounts and main accounts. Then you need to define the dimensions and dimension sets, followed by the accounting structures. Finally, you need to set up the ledger, where you link the fiscal year, chart of accounts, and accounting structure. You also need to define the default currency and default exchange rate in the ledger setup. All your accounting transactions follow the configuration you have implemented in the ledger setup.

Accounts receivable:

Accounts receivable (AR) is the balance of funds due to a customer for products or services delivered and invoiced. The total value of all accounts receivable is listed on the balance sheet as current assets. AR is used to track customer invoices and incoming payments. You can

create customer invoices that are based on sales orders or packing slips. You can create free text invoices if the invoices aren't related to sales orders. You can also receive payments by using several payment types, which include bills of exchange, cash, checks, credit cards, and electronic payments.

Use case You need to account for all the receivables transactions in your ledger book, such as customer invoices and vendor returns. The Accounts receivable module can settle all your receivables with the payment transactions. The module supports different modes of payments, payment terms, cash discount rules, payment days, and calendars.

Accounts payable:

Accounts payable (AP) are the amounts of money that a company owes its vendors or suppliers for goods or services that have been received but not yet paid for. The total value of all accounts payable is listed on the balance sheet as the liability. You can manually enter vendor invoices or import them electronically through integration services. After invoices are entered or received, they can be reviewed and approved by using an invoice approval journal. The system enables the use of invoice matching, vendor invoice policies, and workflows to automate the review process. Invoices that meet certain criteria are automatically approved and the remaining invoices are flagged for review.

Use case: You need to account for all the payable transactions in your ledger book, such as vendor invoices and customer returns. The Accounts payable module can settle all your payables with the payment transactions you make. The module supports different modes of payment, such as check and electronic payment, payment terms, cash discount rules, payment days, and calendars.

Cost accounting:

Cost accounting is a branch of accounting that deals with the process of recording, classifying, analyzing, and summarizing the costs incurred by a business. The Cost accounting module manages the processes used in cost accounting, such as allocation base, cost accounting ledger, cost entry, cost classification, and cost behavior.

Use case: You're the regional operations head of a multinational company. You're responsible for the operations of four countries, represented by four different legal entities. You have a cost center to manage the operations of the countries. The Cost accounting module helps you account for the day-to-day operations of the legal entities. It helps you decide how to effectively use the resources by tracking and measuring them and studying their effects. It also guides you toward cost control.

Budgeting:

This module provides an overview of the budgeting functionality components, budgeting tools, and reporting capabilities. The budget module in Dynamics 365 is divided into three primary sections: budget planning, budget entry, and budget control. Budget planning is the process that ensures the organization policies, procedures, and requirements are met while implementing the budget. Budget entry, the following step, helps register the budget line items in Finance and maps the line items with general ledger accounts. Budget control is the optional step that validates the financial transactions in Finance based on the registered budget lines.

Use case: You're the financial controller of an organization. You use Finance to ensure long-term strategic planning and annual budget planning to track financial transactions aligning with the organizational hierarchy. Budget allocation can be configured for the main accounts and dimensions defined in the chart of accounts of the organization. You can also enforce budget control at the transaction level, based on the established budget. The level of control depends on the organizational culture and the organization's level of maturity.

Cash and bank management:

Cash and bank management is used to maintain the legal entity's bank accounts and the financial instruments that are associated with those bank accounts. These instruments include



deposit slips, checks, bills of exchange, and promissory notes. You can also reconcile bank statements and print bank data on standard reports.

Use case: You can maintain organizational bank accounts and perform all bank-related operations using this module. If you need to reconcile a bank statement with your ledger book, Finance allows you to import the bank statement that can be automatically reconciled from within bank transactions. You can also forecast the cash flow figures in this module. The account payables and receivables data along with the payment conditions can deduce the cash flow forecast of your organization.

Fixed assets:

This module provides access to resources that use fixed assets for Finance. Fixed assets are items of value that are owned by an individual or organization. The items include buildings, vehicles, land, and equipment.

Use case: Different organizations have different types of fixed assets to run their business. There are tangible assets, such as property, equipment, and inventory. You use these fixed assets to produce goods and services for the organization. You also have intangible assets, which don't exist physically but represent a monetary value, such as copyrights, brands, and goodwill. This type of asset can add to an organization's future value and worth and can sometimes be more valuable than the tangible assets. In the fixed assets module, you maintain an asset's profile, such as purchase details, current valuation, and depreciation profile.

Expense management:

Expense management can create an integrated workflow to store payment method information, import credit card transactions, and track the money that employees spend. You can also define expense policies and automate the reimbursement of travel expenses.

Use Companies: Your company has rules and policies defined for different expenses such as travel and food. In the expense management module, you can define all these policies based on the organizational hierarchy. For example, when an employee books expenses, they are aligned with the entered policies. It's also possible to enter expenses for cross-legal entity scenarios, when an employee is engaged in a project that belongs to a different legal entity and expenses are required to be entered against that project.

Regulatory features:

Finance and operations apps include regulatory functionality for different countries/regions. This functionality is enabled based on the primary address of the active legal entity. There are

regulatory updates to this functionality to address new or changed country-specific or region-specific legislation. Regulatory updates that are delivered either as hot fixes or as part of a release preview can be identified by the abbreviations HF and Preview, respectively. It also submits and reviews regulatory alerts. You can check Regulatory updates for the latest regulatory update plans.

Use case: You're an accountant in an organization in India. You need to implement the Goods and Service Tax (GST) in the electronic invoices created for your local customers. You can use the Regulatory features module to accomplish this by downloading and implementing the Electronic Invoice under GST hotfix, which provides India-specific regulatory updates.

Asset leasing:

Finance provides an advanced capability for managing, tracking, and automating financial transactions for leased assets. This module can capture and process the lease details and generate journal entries throughout the lifecycle of the lease, from initial recognition to monthly journal entries, to impairment and termination of the lease.

Use case Your company plans to purchase furniture for renting to customers. You need to first procure the furniture using the Procurement and sourcing module, followed by converting the furniture to fixed asset. The asset leasing process includes transactions such as lease agreements, lease calculations, and lease transactions, which are booked in the ledger book in accordance with the defined posting rule. Finance enables the company to maintain this process along with various lease components such as payment schedules, start and end dates, payment frequency, and lease amortization.

Revenue recognition:

Companies that sell multiple product types, such as products, services, and subscriptions, must be able to break out multi-element orders so that revenue can be recognized based on a set of company-specific and industry-specific guidelines. In general, the revenue recognition process can be used to perform two basic tasks: allocate revenue and defer revenue. Allocate revenue ensures that the appropriate revenue price is recognized, based on the value of the components on multi-element orders. Defer revenue represents the contractual time frame and percentages for recognizing revenue over time.

Use case: You work as an accountant in an organization that sells products and services. A sales executive sold a TV with an installation charge and annual maintenance contract. The installation takes place the following month. Therefore, at the time of the posting of the sales order, only the revenue of the product gets recognized. The revenue of the installation service gets recognized the following month when the installation actually happens. For the revenue from the maintenance contract, every month one-twelfth of the total revenue will be recognized until the next year.

Credit and collection management:

Customer credit management lets you manage credit limits and control the flow of sales orders through the posting process, based on credit rules that you create. Collections management provides a centralized view where accounts receivable collections information is managed. The accounts receivable module provides the payment terms and schedules, which define the collection generation process. It can generate collection reminders based on the defined scheduled. It can also generate interest if there's payment due.

Use case: You are in a sales organization, responsible for maintaining relationships with customers and generating sales orders. You can use the credit management module to find eligibility levels of customers based on their credit score. Collection managers can use the centralized view to manage collections. Collections agents can begin the collections process either from customer lists that are generated by using predefined collection criteria or from the Customers page.



3.3. DESCRIBE ORGANIZATION AND LEGAL ENTITIES

Creating a legal entity and preparing it for financial management is the first phase of implementation.

A legal entity is an organization that has a registered or legislated legal structure. Legal entities can enter into legal contracts and are required to prepare statements that report on their performance. The country or region that you select for the primary address of the legal entity controls the country-specific and region-specific features available for the legal entity.

Before choosing the country/region for the new legal entity, you need to understand the significance of localization in finance and operations apps.

Some regulatory requirements of certain countries/regions require that finance and operations apps enable or disable certain functionality and features, and even some forms, fields, reports, and inquiries.

A company is a type of legal entity. In Dynamics 365 Finance, companies are the only kind of legal entity you can create, and every legal entity is associated with a Company ID.

The Company ID field is limited to four alphanumeric characters. Once it is created, it cannot be changed. So, be sure to properly plan for and consider a naming convention prior to creating legal entities in the production environment. Users can access data only for the company that they are currently signed in to and have security access for the roles they belong to.

A search name is an alternate name that can be used to search for this legal entity. One of the best ways to learn about finance and operations apps and be able to successfully implement them is by listening to the story of a customer's day-to-day operations. You need to be able to gather and convert the customer requirements into test cases and try to match the functionality and configuration of finance and operations apps with the customer's business processes.

Example:

Contoso is an organization that has at least one company or legal entity and has registered its international companies in multiple countries, such as Germany, United States, and France. Therefore, Contoso is an organization that is a group of people who are working together to carry out a business process or achieve a goal. Organizational hierarchies represent the relationships between the organizations that make up your business. This organization has decided to acquire a business named Adventure Works Cycles. You can create a new legal entity by navigating to the Legal entities page.

Registration IDs:

Many countries and regions have different regulations and requirements for recording registration numbers or IDs.

For different countries/regions, there are various location-specific functionalities related to registration numbers provided by different government offices. Examples of registration numbers include employer identification number (EIN), tax identification number (TIN), and European value added tax (VAT) identification (EU VAT ID). This feature provides a unified framework for all countries and regions with consideration of country-specific and region-specific requirements of some European countries.

The Registration category is a country/region registration identifier approved for use in a country/region for tax, customs, and other purposes.

After you create the legal entity, the next step is to configure number sequences for the newly created company. Number sequences are used to generate and manage unique identifiers for the master and transaction data required to manage uniqueness.

Move on to the next section to learn how to handle regional tax reporting requirements.

3.4. DESCRIBE NUMBER SEQUENCE FUNCTIONALITY

After configuring different components of the organization, your next step is to configure number sequences for the newly created company.

The number sequence framework in finance and operations apps can generate and manage unique identifiers for different types of records throughout the system. The identifiers can be associated to master data or transaction data.

Number sequence also helps to define the format of the identifier, which may include a prefix or numbering convention. Some identifiers may need to include the legal entity or operating unit as a prefix. Some might require the fiscal year as a part of the identifier. You can define this in the Segment section of the number sequence.

Scope:

The scope of the number sequence helps to identify the components available in the Segment sections, such as legal entity and fiscal year. Following are the possible scopes of a number sequence:

Shared: There are tables in finance and operations apps for which records aren't legal entity

specific, such as product and global address book. If you need to add a number sequence for such a table, the scope should be shared. In a shared number sequence, you can't have a legal entity or fiscal year as a prefix.

Company: For the legal entity-specific tables, you can define a number sequence for a specific legal entity that you need to select while creating the number sequence. For the company-scoped legal entities, you have the legal entity as a segment, which will enable you to include the legal entity in the identifier.

Company and fiscal calendar period: With the legal entity, if you need to add the fiscal year as a part of your transaction identifier, you should use the company and fiscal calendar period as the number sequence scope. It adds the fiscal year in the Segment section that enables the fiscal year and company to be prefixed in the identifier.

Legal entity: The tables of finance and operations apps have a standard field named `dataAreaId`, which is automatically created when a table is created. This field contains the legal entity to which a specific record belongs. If the number sequence scope is Company, a new number sequence is created based on the legal entity in the `dataAreaId` field.

There are some tables in finance and operations apps, such as Travel Expense, that contain another field that also refers to the legal entity information. For example, a non-US employee who is working on a US project records expenses against that project. When the employee enters an expense, the `dataAreaId` field is populated with the non-US legal entity. However, the second legal entity field holds the US legal entity information. If the number sequence should be created based on the second legal entity field, which isn't the `dataAreaId` field, then you need to use legal entity as the scope of the number sequence.

You have the option in the segment to select the legal entity as a part of the identifier.

Legal entity and fiscal calendar period: If you need to add the fiscal year along with the second legal entity field (as described in the preceding "Legal entity" paragraphs) as the prefix of the transaction identifier, you should use Legal entity and fiscal calendar period as the scope of the number sequence.

Operating unit type: There are five standard operating unit types available in finance and operations app: business unit, department, cost center, value stream, and commerce channel. You can have a number sequence defined based on the selected operating unit types. This enables you to create a prefix based on the operating unit type in the segment area.

Operating unit: This option is mostly applicable for the commerce store functionality. You can enable a number sequence for the store-specific transaction by using operating unit as the scope. In this number sequence, you can have the store number as a part of the transaction identifier by including it in the segment section.

Continuous number sequence:

Number sequences can be continuous or noncontinuous. A continuous number sequence doesn't skip any numbers. If there's a noncontinuous number sequence, there's the possibility that some numbers might be skipped. For example, if a user cancels a transaction, a number might be generated but not used. In a continuous number sequence, that number is recycled. In a noncontinuous number sequence, the number isn't used. In a continuous number sequence, during assigning a new number, the system needs to check if the preceding number is skipped. Because of this extra algorithm, continuous number sequences often encounter performance issues.

Number sequence:

It's critical to select the correct number sequence because an incorrectly configured number sequence impacts the performance of the page.

3.5. DESCRIBE TAX CAPABILITIES**Sales tax groups:**

Sales tax groups are groups of sales tax codes that are attached to customers and vendors. They're also attached to ledger accounts for transactions that aren't posted to a vendor or customer.

A sales tax group includes all sales tax codes that apply when you trade goods or services with customers and vendors, as depicted in the screenshot:

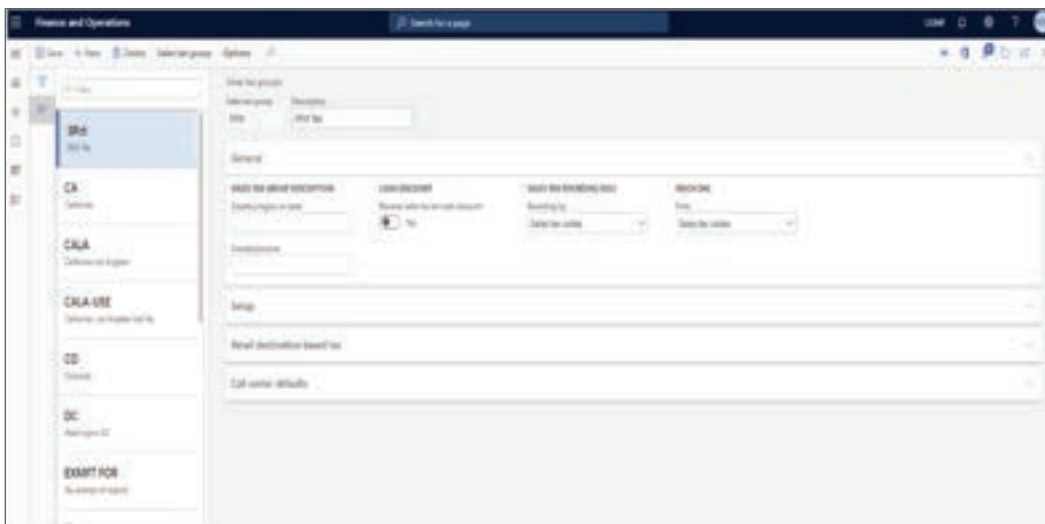


Figure 3.2.A page for sales tax groups.

In most countries or regions, different tax rules apply when you trade with domestic and foreign customers. The tax rules for foreign trade are frequently split up based on bilateral and multilateral trade agreements. Therefore, you need to create tax groups depending on the taxes that might apply for a certain group of customers or vendors.

A careful analysis of the different types of customers and vendors that the company trades with is a good starting point for determining the types of sales tax groups needed and the setup of those sales tax groups.

Because the geographic location of the customer or the supplier determines taxes, you usually assign the same sales tax group to similar trading partners in the system. The correct tax codes the system uses are attached to this sales tax group.

Item sales tax groups:

Because items generally determine taxes, you need to indicate how taxes are calculated for each item.

Item sales tax groups are groups of sales tax codes that are attached to resources like products. The item sales tax group includes all the sales tax codes that apply when you sell that item. The item sales tax group also might include most of the sales tax codes in the system. When you create the item sales tax groups, you attach the group to items.

The sales taxes that apply to a particular transaction are determined by the sales tax codes that are included in both the sales tax group and in the item sales tax group of the transaction. Sales tax can be calculated only if a sales tax group and an item sales tax group are selected for each transaction for which sales tax must be calculated or recorded. The following screenshot depicts the Item sales tax group page.

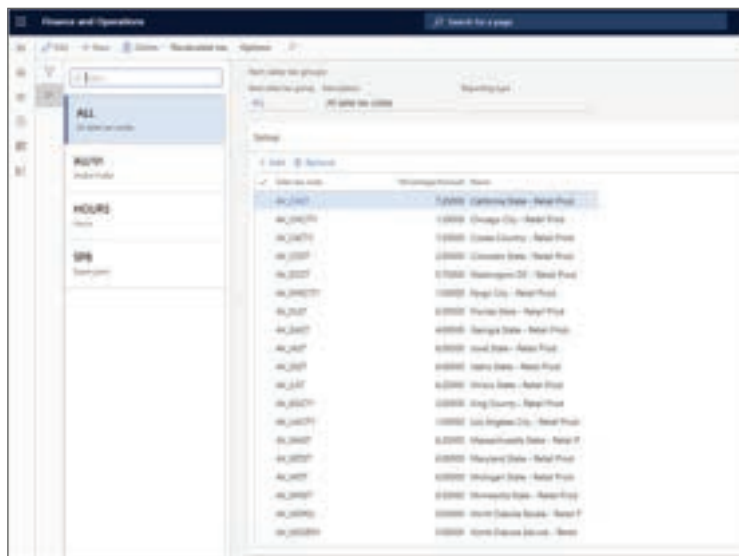


Figure 3.3. The Item Sales Tax Group view.

Note:

Every transaction for which sales tax needs to be calculated and posted must have a sales tax group and an item sales tax group.

Sales tax groups are related to the party (for example, customer or vendor) of the transaction, whereas item sales tax groups are related to the resource (for example, item or procurement category) of the transaction. Tax groups contain a list of tax codes. The tax codes that are present in both the sales tax group and item sales tax group for a transaction are the tax codes that apply to that transaction.

Sales tax reporting codes:

Sales tax reporting codes refer to a field number on a sales tax report. They're used on country-specific or region-specific report layouts and the Sales tax payment by code report to print sales tax amounts for a settlement period that is summarized for each reporting code.

Sales tax must be reported and paid to tax authorities at regulated intervals (monthly, quarterly, etc.). Finance provides functionality that lets you settle tax accounts for the interval and offset the balances to the tax settlement account, as specified in the ledger posting groups. You can access this functionality on the Settle and post sales tax page. Make sure you specify the sales tax settlement period that sales tax should be settled for.

After you create Sales tax reporting codes, you can refer to them on the Report setup FastTab in the Sales tax code page.

This layout is used to filter the available reporting codes for a sales tax code. Each sales tax code belongs to a settlement period that belongs to a sales tax authority that uses a report layout.

After the sales tax has been paid, the balance on the sales tax settlement account should be balanced against the bank account.

If the sales tax authority specified on the sales tax settlement period is related to a vendor account, the sales tax balance is posted as an open vendor invoice and can be included in the regular payment proposal.

The following is a sample of the Sales tax code report for Contoso Entertainment System:

The screenshot shows the 'Sales tax reporting codes' report in Microsoft Dynamics 365. The report is for 'Contoso Entertainment System Germany' and is titled 'Sales tax reporting codes'. It displays three sections for different sales tax codes: EU8, EU19, and EU7. Each section includes a table with columns for 'Sales tax code', 'Name', 'Settlement period', and 'Report layout'. The tables list various reporting codes such as 'Taxable sales', 'Tax-free sales', 'Sales tax on purchases', 'Taxable purchases', 'Tax-free purchases', 'Sales tax receivable', 'Taxable import', 'Other taxable import', 'Use tax', and 'Other use tax'. The report also shows 'Sales tax on sales credit note' and 'Tax exempt purchase credit note' for each code. The interface includes a search bar at the top, navigation icons on the left, and a page number 'Page 1' with the date '10/16/2019' and time '12:12 AM' in the top right corner.

Figure 3.4. The Sales tax code report for Contoso Entertainment System.

You can take what you learned in this unit and expand it by learning about cost accounting concepts.

Sales tax configuration:

This sales tax configuration is applicable for the transactions in Dynamics 365 Supply Chain Management and Dynamics 365 Commerce also.

3.6. DESCRIBE COST ACCOUNTING CONCEPTS

Cost accounting is a form of managerial accounting that aims to capture a company's total cost of production by assessing the variable costs of each step of production, and fixed costs, such as a lease expense.

Cost accounting in Finance provides important insights into the cost efficiency and capacity of the managerial decision-making processes. It empowers cost controllers and cost center managers to control, classify, allocate, and analyze costs of current operations and plan for future changes.

The analysis content in the cost accounting module highlights variances between the actual costs and budgeted costs. Based on the analysis, managers can be notified about positive and

negative trends for their operational units. Managers can drill down to the cost element hierarchies or individual cost elements. In this way, managers can gain detailed insight into how cost variances have occurred, and then take effective action.

The Cost control workspace in Cost accounting > Cost control is designed as a page. Therefore, all managers who are responsible for a cost object can be granted access. You can control access to the page and data in the form. Control the list of reports available for users, such as managers, by setting the Published option on the Cost control workspace configurations page.

A manager can select the fiscal calendar period to view. The session date is used to determine the default current period. The values in the fiscal calendar period are determined by the report name and the fiscal calendar selected for the cost accounting ledger that is associated with the report name on the Cost control workspace configurations page.

In the cost object dimension hierarchy, users can select the aggregation level at which balances should be displayed. By enabling access-level security, you control the permissions so users can view the entire hierarchy. However, users are only able to view balances for chief officers, such as the CEO and CFOs, who have been granted access.

Users can customize the columns on a report to fit their requirements. The customizations affect only the user that makes the changes after the new format is saved.

Users can drill into the details behind the balances included in the workspace, as depicted in the following screenshot. If users select a cost element dimension hierarchy node, and then select View details, the Cost element details dialog box displays detailed information for the node.

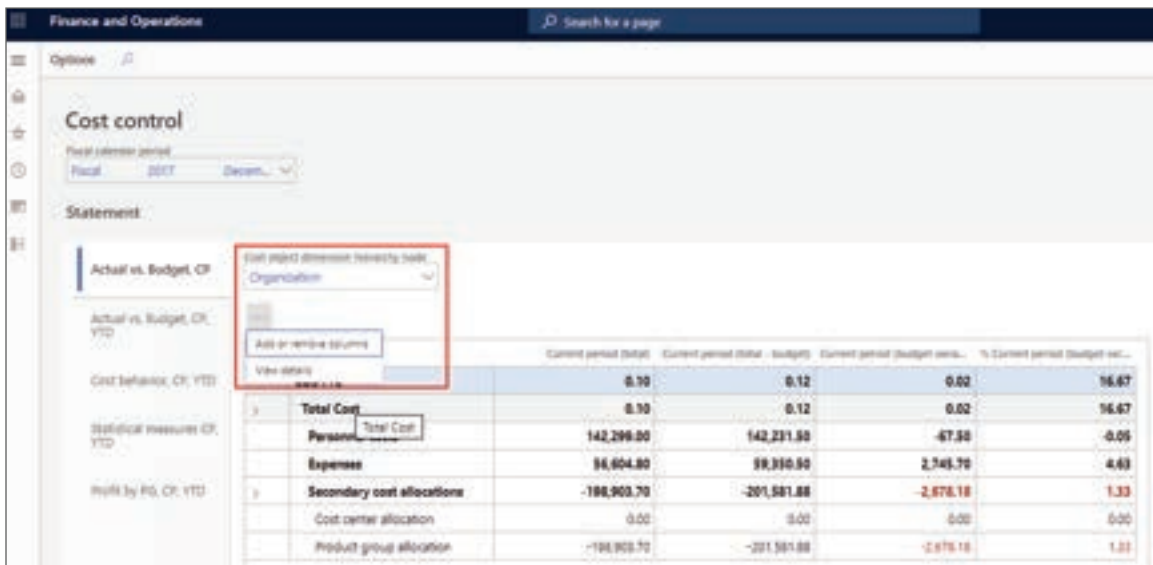


Figure 2.1.5. The Cost Control Window. The View details function is highlighted.

A grid displays each cost element that is associated with the cost element dimension hierarchy node and its values, as depicted in the following screenshot. The columns that appear in the grid match the workspace settings. Two charts present a summary of actual versus budget and budget variance by period.



Figure 2.1.6. The cost element details of the CDS P/L page. A summary of actual versus budget and budget variance by period is displayed.

Users can select Cost entries to drill down into the entry details as required, depicted in the following screenshot, by selecting View details and then selecting Cost entries in the Cost accounting > Cost control workspace.

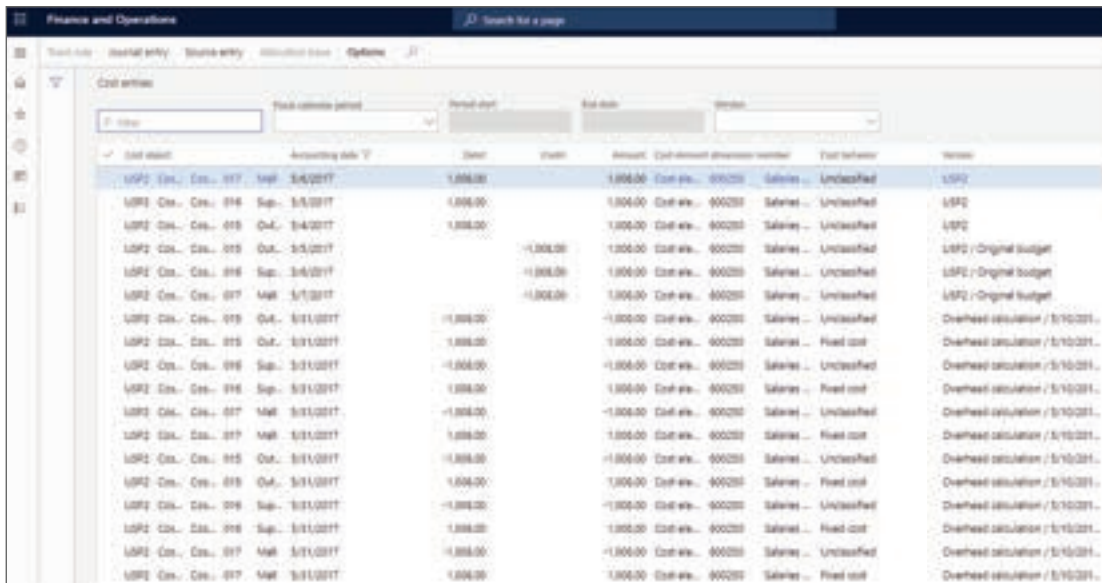


Figure 2.1.7. The Cost entries view and allows users to drill down into the entry details.

For example, rent is an expenditure that is distributed to cost centers. Users who want to understand the rent cost that their cost center must carry can drill down to view how rent has been calculated.



SUMMARY

Here's a concise summary:

Finance Capabilities and Features:

- Finance is designed for multi-company, multi-currency organizations, offering real-time performance monitoring and data-driven decision-making.

Modules:

- General Ledger: Manages financial records, chart of accounts, and more.
- Accounts Receivable: Tracks customer invoices and payments.
- Accounts Payable: Manages vendor invoices and payments.
- Cost Accounting: Records, analyzes, and controls business costs.
- Budgeting: Supports budget planning and control.
- Cash and Bank Management: Maintains bank accounts and reconciliations.
- Fixed Assets: Manages tangible and intangible assets.
- Expense Management: Streamlines expense workflows and policies.
- Regulatory Features: Ensures compliance with country-specific regulations.
- Asset Leasing: Automates lease management.
- Revenue Recognition: Allocates and defers revenue based on sales.
- Credit and Collection Management: Manages credit limits and collections.

Organization and Legal Entities:

- Legal entities are registered entities with specific legal structures.
- Each legal entity has a unique Company ID.

Number Sequence Functionality:

- Number sequences generate unique identifiers for various records.
- They can have different scopes, including shared, company-specific, and more.

Tax Capabilities:

- Sales Tax Groups group tax codes for customers and vendors.
- Item Sales Tax Groups determine taxes for items.
- Sales Tax Reporting Codes are used for tax reporting.
- Sales tax can vary based on customer type and location.

Cost Accounting Concepts:

- Cost accounting records variable and fixed costs.
- It helps analyze cost variances and budget performance.
- Managers can drill down into cost details for better insights.

MULTIPLE CHOICE QUESTIONS (MCQ) FOR PRACTICE

- 1 What is the primary purpose of the Finance module described in the content?
 - a) Inventory management
 - b) Human resource management
 - c) Financial performance monitoring
 - d) Customer relationship management
- 2 How does the General Ledger module help organizations manage their financial records?
 - a) It tracks customer invoices.
 - b) It manages employee payroll.
 - c) It maintains legal entity financial records.
 - d) It handles sales order processing.
- 3 Which module is responsible for tracking customer invoices and incoming payments?
 - a) General Ledger
 - b) Accounts Receivable
 - c) Accounts Payable
 - d) Cash and Bank Management
- 4 What is the primary function of the Cost Accounting module?
 - a) Managing customer relationships
 - b) Analyzing financial variances
 - c) Handling inventory transactions
 - d) Maintaining employee records
- 5 Which module assists in long-term strategic planning and annual budget planning?
 - a) Cash and Bank Management
 - b) Budgeting
 - c) Fixed Assets
 - d) Expense Management
- 6 What does the Cash and Bank Management module allow organizations to forecast?
 - a) Employee salaries
 - b) Customer invoices
 - c) Cash flow figures
 - d) Vendor payments

- 7 What types of assets are typically managed in the Fixed Assets module?
- a) Employee assets
 - b) Customer assets
 - c) Tangible and intangible assets
 - d) Vendor assets
- 8 Which module helps organizations track and automate financial transactions for leased assets?
- a) Budgeting
 - b) Expense Management
 - c) Asset Leasing
 - d) Revenue Recognition
- 9 What is the primary purpose of the Revenue Recognition module?
- a) Managing customer relationships
 - b) Allocating revenue
 - c) Deferring revenue
 - d) Recognizing revenue based on guidelines
- 10 Which module helps organizations manage customer credit limits and collections?
- a) Budgeting
 - b) Cash and Bank Management
 - c) Credit and Collection Management
 - d) Expense Management
- 11 What is a legal entity in the context of financial management?
- a) A financial statement
 - b) A registered or legislated legal structure
 - c) A financial transaction
 - d) An organizational hierarchy
- 12 Why is it important to select the correct number sequence in financial management?
- a) To create financial reports
 - b) To control access to data
 - c) To improve customer relationships
 - d) To avoid performance issues
- 13 What does the scope of a number sequence determine in financial management?
- a) The number of users who can access it
 - b) The format of the identifier
 - c) The level of security
 - d) The reporting capabilities

- 14 What is the role of Sales Tax Groups in financial management?
- a) Managing employee taxes
 - b) Managing vendor invoices
 - c) Calculating taxes for customers and vendors
 - d) Managing cash flow
- 15 What does the Cost Accounting module help managers analyze?
- a) Customer relationships
 - b) Financial performance
 - c) Human resource management
 - d) Inventory management

Answers

- 1 C. Financial performance monitoring
- 2 C. It maintains legal entity financial records.
- 3 B. Accounts Receivable
- 4 B. Analyzing financial variances
- 5 B. Budgeting
- 6 C. Cash flow figures
- 7 C. Tangible and intangible assets
- 8 C. Asset Leasing
- 9 D. Recognizing revenue based on guidelines
- 10 C. Credit and Collection Management
- 11 B. A registered or legislated legal structure
- 12 D. To avoid performance issues
- 13 B. The format of the identifier
- 14 C. Calculating taxes for customers and vendors
- 15 B. Financial performance

**SELF-EXAMINATION QUESTIONS FOR PRACTICE:**

- 1 What is the primary purpose of the Finance module described in the content?
- 2 How does the General Ledger module help organizations manage their financial records?
- 3 Describe the key functions of the Accounts Receivable module.
- 4 What are the benefits of using the Cost Accounting module in finance?
- 5 Explain the role of the Budgeting module and its components in financial management.
- 6 How does the Cash and Bank Management module assist in financial operations?
- 7 What types of assets are managed in the Fixed Assets module, and why are they important?
- 8 How does the Regulatory Features module help organizations ensure compliance with regulations?
- 9 Describe the purpose of the Sales Tax Groups and Item Sales Tax Groups in tax management.
- 10 What role does cost accounting play in analyzing financial performance and variances within an organization?

CHAPTER 4

DESCRIBE THE GENERAL LEDGER IN DYNAMICS 365 FINANCE



LEARNING OBJECTIVES

- Describe chart of accounts, including main accounts and classification.
- Describe financial dimensions and dimension set concepts.
- Describe periodic financial processes.
- Describe journaling concepts.

4.1. INTRODUCTION

Finance provides fast, dependable, and comprehensive accounting, financial reporting, and analysis. It manages the accounting processes involved in classifying, sorting, storing, and summarizing financial transactions related to company's assets, liabilities, and capital.

In this module, you discover the chart of accounts, and then explore the various types of financial dimensions and how they're set up. You also look at periodic financial processes, such as financial period closes, year-end 1099 reporting, and financial consolidation.

4.2. DESCRIBE THE CHART OF ACCOUNTS FUNCTIONALITY

Introduction to the chart of accounts:

A chart of accounts (COA) is an index of all the financial accounts in the general ledger of a company. In short, it's an organizational tool that provides a digestible breakdown of all the financial transactions that a company conducted during a specific accounting period, separated into subcategories.

Configure ledger and journal setup:

You can use journals quickly and efficiently once they're set up. Several components must be set up to use general journals.

Ledger:

Each legal entity has one ledger, and each ledger can be linked to one chart of accounts. Multiple ledgers can be linked to the same chart of accounts, which allows you to share the same chart of accounts with more than one legal entity. You also need to indicate which account structure or structures to attach to the ledger for each legal entity.

Balancing financial dimension:

Interunit accounting is the requirement that you generate a balance sheet for a specific financial dimension. Therefore, all accounting entries made to the general ledger must be balanced for the values of the financial dimension, which is referred to as the balancing financial dimension. The balancing financial dimension used for interunit accounting is selected on the Ledger page in General ledger > Ledger setup > Ledger. When you enter the balancing financial dimension in Finance, as depicted in the screenshot, every accounting entry must balance at the total level and at the level of the financial dimension values.

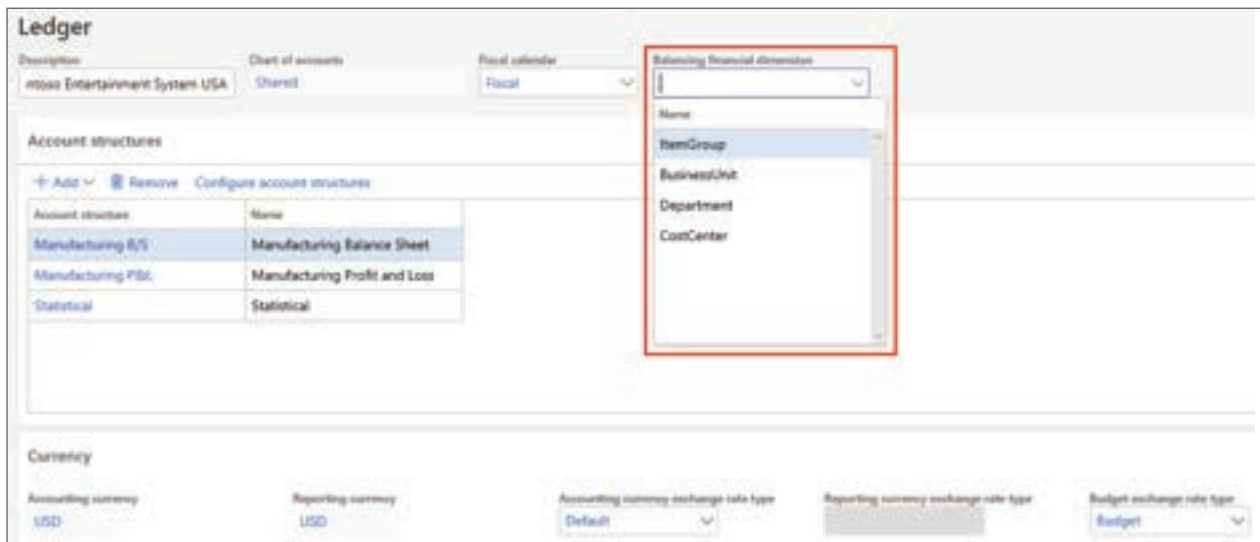


Figure 4.1. The Ledger page. The Balancing financial dimension section is highlighted.

If the accounting entry doesn't balance at the level of the financial dimension values, other accounting entries are created automatically to balance the accounting entry.

After adding account structures, you'll want to link them to the ledger.

The ledger rules are applicable to all the financial transactions in the selected legal entity.

Journal setup:

Finance includes manually generated journals and system-generated journals.

Examples of system-generated journals are the journals that come from the subledgers of Accounts receivable and Accounts payable.

Manual journal entries are generated by postings entered into the system, such as a monthly recurring insurance expense or a one-off redistribution of revenue across departments. When

you use a manual journal entry, the transactions aren't posted immediately. Before you can post a manual entry, journals can be in the following states:

- Changed
- Reviewed
- Approved
- Deleted

Journal approval is optional.

In Finance, you can use journals to do the following tasks:

- Control different kinds of entries - You can apply an approval system so that special journals are posted only after they're approved.
- Review data imported from external ledger systems - You can ensure that all valid fields contain a value and that all restrictions for the transaction are fulfilled.

You should make sure that the necessary voucher series is set up before you create journals. You can set up number sequences and attach them to the appropriate references.

You can't use both the manual approval system and the workflow approval system for the same journal name. You can use the following posting layers:

- Current - Default layer that is used
- Operations - Used for entry of transactions
- Tax - Where you record transactions that impact tax reporting

In the Detail level list, you can specify how journal lines should be summarized.

- Details - Every instance of an account number in the journal lines is posted as a separate account transaction.
- Summary - A summation of journal lines into one transaction is performed automatically during posting if voucher with date, account number, dimension, and currency code contain the same values.

It's important to know that the summation isn't performed on transactions with sales tax.

Transaction types:

You can add other text to default descriptions for transaction types related to the following document types:

- Customer invoices
- Customer credit notes
- Customer cash payments
- Vendor payments

- Sales orders
- Purchase orders
- Inventory journals
- Master planning (MRP)
- Fixed assets

Continue on to explore financial dimensions and dimension set concepts.

4.3. DESCRIBE FINANCIAL DIMENSIONS AND DIMENSION SET CONCEPTS

Financial dimensions

This unit explains the various types of financial dimensions and how they're set up.

The Financial dimensions page contains the segments in your accounting structure, which is critical for reporting purposes.

Use the Financial dimensions page to create financial dimensions you can use as account segments for chart of accounts. There are two types of financial dimensions: custom dimensions and entity-backed dimensions. Custom dimensions are shared across legal entities, and the values are entered and maintained by users. For entity-backed dimensions, the values are defined somewhere else in the system, such as in Customers or Stores entities. Some entity-backed dimensions are shared across legal entities, whereas other entity-backed dimensions are company-specific.

After you create the financial dimensions, use the financial dimension values page to assign more properties to each financial dimension.

You can use create custom financial dimensions to correspond to legal entities. You don't have to create the legal entities in Finance. For example, if you have multiple legal entities, you can create a custom financial dimension to represent an organization. All transactions should be associated to that custom legal entity. This is more commonly used if the implementation is non-finance.

However, financial dimensions aren't designed to address the operational or business requirements of legal entities. The interunit accounting functionality in Finance is designed to address only the accounting entries created by each transaction.

Before you set up financial dimensions as legal entities, evaluate your business processes in the following areas to determine whether this setup works for your organization:

- Inventory
- Sales and purchases between financial dimensions and legal entities
- Sales tax calculation and reporting
- Operational reporting

Some of the limitations include the following:

- You can use sales tax functionality only with legal entities, not with financial dimensions.
- Some reports don't include financial dimensions. Therefore, to report by financial dimension, you might have to modify the reports.

Custom dimensions:

To create a user-defined financial dimension, in the Use values from field, select Custom dimension. You can create a custom dimension for an entity that doesn't exist in Finance.

You can also specify an account mask to limit the amount and type of information that can be entered for dimension values. You can enter characters that remain the same for each dimension value, such as letters or a hyphen (-). You can also enter number signs (#) and ampersands (&) as placeholders for characters that change every time a dimension value is created. Use a number sign (#) as a placeholder for a number and an ampersand (&) as a placeholder for a letter. The field for the format mask is available only when you select Custom dimension in the Use values from field.

Example:

To limit the dimension value to the letters "CC" and three numbers, enter CC-### as the format mask.

Entity-backed dimensions:

To create an entity-backed financial dimension, in the Use values from field, select a system-defined entity to base the financial dimension on. Financial dimension values are then created from that entity. For example, to create dimension values for projects, select Projects. A dimension value is then created for each project name. The Financial dimension values page presents the values for the entity. If those values are company-specific, the page also displays the company.

Activating dimensions:

When you activate a financial dimension, the table is updated so it includes the name of the financial dimension. You can enter dimension values before you activate a financial dimension. However, a financial dimension can't be consumed anywhere until it's activated. For example, you can't add a financial dimension to an account structure until the financial dimension has been activated. When you select Activate, all dimensions are updated and display status changes.

Translations:

On the Text translation page, you can enter text for the selected financial dimension in various

languages. On the Main account translation page, you can enter text for the main account in various languages.

Legal entity overrides:

Not all dimensions are valid for all legal entities. Additionally, some dimensions might be relevant only for a specific period. In these cases, you can use the Legal entity overrides section to specify the companies that the dimension should be suspended for, the owner, and the period when the dimension is active.

Financial dimension sets:

Use the Financial dimension sets page to create financial dimensions. A financial dimension set contains either financial dimensions or financial dimension combinations. The main account is always included and can be combined with other financial dimensions. The main account can also be the only financial dimension included in a financial dimension set.

The order in which financial dimensions in a set are displayed determines how transactions are sorted and fields are printed on reports.

For example, a financial dimension set includes the Department and Cost center financial dimensions. The financial dimension set is set up so that the Department amounts are displayed first on reports, followed by the Cost center amounts.

When you view or report on financial transactions, the financial dimension sets that are defined can be used individually or in pairs. You can select a primary and secondary financial dimension set. The secondary financial dimension set includes more detailed information about the amounts that are in the primary financial dimension set.

4.4. DESCRIBE PERIODIC FINANCIAL PROCESSES

In Finance, you can complete closing procedures for a period, such as a day, month, or year. Closing processes prepare the system for a new period.

Prepare for financial period close:

Each organization has different processes and steps that it performs for the end of a period. Optional steps for period end include:

- Settle invoices and payments.
- Post all transactions for period end.
- Verify that all journals are posted.
- Run foreign currency revaluation for the general ledger to generate any unrealized gain or loss amounts.
- Run foreign currency revaluation for accounts payable and accounts receivable.
- Settle ledger transactions.

- Process any required allocations.
- Reconcile the subledgers to the general ledger.
- Manually post period-end adjustments.
- Journalize transactions and review the Ledger journal report.
- Perform a consolidation by using a consolidation company or financial reporting.
- Generate period-end financial statements by using financial reporting.
- Set ledger periods to On hold so that no further posting occurs. For better control, you can also restrict a period to a specific user group while period-end activities are occurring. As a best practice, don't use the Permanently closed status, because you can't reopen a period that has been set to Permanently closed. This status could be used at a much later time.

Financial period close workspace:

The Financial period close workspace lets you track your financial closing processes across companies, areas, and people. Depending on the security role assigned to your user profile to view the Financial period close workspace, you'll see either all tasks and statuses for a closing schedule or only the tasks that are assigned to you.

You can find the financial period close workspace by accessing General ledger > Workspaces > Financial period close. You can use the workspace to organize and track the tasks that are required for various period-end processes.

You must first select a closing schedule at the top of the workspace. All data presented on the workspace is then filtered by the selected closing schedule.

Summary tiles in the workspace, depicted in the following screenshot, provide an overview of the process, and indicators help you keep the closing process on track. They list out the tasks that are past due, remaining tasks for today, tasks that are due today but are blocked because of dependencies, and all remaining tasks for the process. This information is for all companies that are included in the selected closing schedule.



Figure 4.2. The Financial period close workspace with the summary highlighted.

Year-end 1099 reporting:

If you do business with vendors that are subject to United States 1099 tax reporting, you must track the amount you pay to each vendor and report that information to the US tax authorities at the end of the calendar year. The vendors are typically individuals who aren't employees and who provide services to your organization. You must also send a statement to each 1099 vendor you do business with, informing them of the amount you're reporting to the tax authorities.

For each vendor that you have set up to be a 1099 vendor, the amounts are tracked within Finance throughout the year. On invoice lines, you can use the 1099 box and 1099 amount fields to track 1099 amounts. Even if you don't enter a value in the 1099 amount field, any payment that is posted for the invoice amount contributes to the 1099 total for the specified 1099 box. If you do enter a 1099 amount, the amount you entered is used instead of the posted payment amount. Finance can process the 1099-MISC, 1099-DIV, 1099-INT, 1099-S (Proceeds from Real Estate Transactions), and 1099-G (Certain Government Payments) information. You can pay an invoice with 1099-G and 1099-S information and process 1099-G and 1099-S tax statements.

Month-end closing:

Let's go through a demo that explains how to process month-end close.

Process year-end close:

At year-end, it's necessary to complete the following tasks:

- Make adjustment entries that reflect transactions from the previous year.
- Print reports, including financial statements.
- Back up data.
- Create a new fiscal year, and transfer opening balances.

Create and post a closing sheet:

A company might print a trial balance sheet to look for inconsistencies and make any adjustments necessary before closing the period. To make adjustments in Finance, you can perform either of the following tasks:

- Make typical journal entries, depending on adjustment.
- Use the Closing period adjustments page.

Consider the following information when you use the Closing period adjustments page:

- It presents an advanced view of the balances on accounts, and you can perform year-end postings directly from it.
- The postings to the page typically occur in the closing period of the fiscal year.

- You can create several specific closing sheets (for revenue, expenses, balance accounts, and so on) and then load the balances from the General Ledger into the closing sheet. After you load the transactions, make transfers from one account to another.
- It resembles a journal, because you can create as many new closing sheets as needed, and you can post several lines of entries.

It's not possible to make transactions to the Opening period in a closing sheet; use the Opening option only for a beginning balance transaction. You can make adjustments, however, to the regular period(s) and to the closing period(s). Usually, this field is set to Closing.

Which columns are populated depends on the Close option that is selected when you set up each account in the chart of accounts.

Post the closing period adjustment:

After you complete the necessary transfers or adjustments, select the Post button to post the closing period adjustment. The closing period adjustment only posts to the closing period.

At this time, you should also run reports and verify results before closing the period and transferring ending balances into the new year as opening balances.

To post the closing sheet, open the closing period on the Periods page. After you post the closing sheet, ensure that you change the period back to On hold.

Financial reporting:

Reporting allows users to create, maintain, deploy, and view financial statements. It moves beyond traditional reporting constraints to help you efficiently design various types of reports.

Financial reporting includes dimension support to determine which financial dimensions you want to include, and the sequence, and it enables you to build a custom reporting structure.

You can map the following to gain better insight of financial data:

- Main accounts
- Financial dimensions
- Combinations of the two

For example, you can create financial row structures to focus on cost accounts. You can set up unlimited financial dimensions that allow for cost detail. The following financial dimensions are examples that might be associated with cost accounts:

- Cost centers
- Departments
- Combinations of the two

Year-end close:

At the end of a fiscal year, you must run the year-end close process to transfer opening balances to the new year. Most companies run the year-end close process multiple times. The first time would be to move the balances into the new fiscal year. The year-end close can then be run again, as many times as required, to move the balances from adjusting entries into the new fiscal year.

Two types of possible transactions are created during the year-end close process. An Opening transaction is always generated and is used to create the opening balances in the new fiscal year. The Opening transaction presents the balance sheet ledger account balances in the new fiscal year and balances from the profit and loss ledger account balances in the retained earnings ledger account in the new fiscal year. The Closing transaction is optionally created to bring the balances of the profit and loss accounts down to zero in the fiscal year that is being closed.

Perform financial consolidation:

In a consolidation, it's possible to gather transactions from several company accounts into a single set of company accounts. You can print reports, such as financial statements, from the consolidation company, but you can't use this company for daily transactions.

Before you perform a consolidation at the close of a period, ensure that the period-closing preparatory activities are performed, but don't close the subsidiary accounts until the consolidation is complete.

You can consolidate data from companies with databases that are external to the consolidation company database, or you can consolidate data from companies in the same database, a so-called "online" consolidation.

Consolidations don't necessarily require that you set up the consolidation company in advance. However, if you want to use the consolidation conversion principles to convert subsidiary data in foreign currencies, you must set up the consolidation company main accounts.

To prepare a consolidation company (the company that collects the results and balances of the subsidiaries), you should have a legal entity created with the Use for financial consolidation process option enabled. Like any other legal entity, you should complete the General ledger module configuration for the consolidation company.

To learn more about configuring the General ledger module, access the corresponding link in the Summary unit at the end of this module.

Intercompany eliminations:

Elimination transactions are required when a parent company conducts business with one or more subsidiary companies and uses consolidated financial reporting.

Some transactions that occur between the companies must be eliminated because consolidated financial statements must only include transactions that occur between the consolidated entity and the other entities that are outside the consolidated group. Because of this requirement, transactions between a parent company and its subsidiary companies must be removed or eliminated.

Predefined elimination rules create elimination transactions in a company that is specified as the destination company for eliminations. You can generate the elimination journals during the consolidation process or by using an elimination journal proposal.

4.5. DESCRIBE JOURNALING CONCEPTS

The purpose of a journal entry is to record a business transaction in an accounting book. A journal entry is recorded in the general ledger. The general ledger is then used to create financial statements for the business.

Based on the type of business transaction, different journal types can be configured in Finance. The Journal names page can be used to set up journals that can be used throughout Finance.

Journal names:

The most important area to set up in the finance module is Journal names, depicted in the following screenshot. Specific journal names should be configured for each purpose, such as intercompany, accrual adjustment, and error correction. You can configure each journal name to ensure data entry for each purpose. Journal names can also be used for reporting purposes.

Figure 4.3. Screenshot depicts the Journal names page of the Finance module.

On the Journal names page, you can set up the following elements:

- Workflow approval – To increase internal control, define journal workflows that establish limits for review and approval steps, based on criteria such as total debit amount. You set up workflows for the general journals on the General ledger workflows page.
- Default values – Select default values for offset accounts, currency, and financial dimensions.
- Journal control – You can set up restrictions on the company and account type, and also the segment values.

The following journal types are some of the more commonly used financial journals available in Finance.

Budget journal:

You can use the budget journal type to process budget appropriations. To use this journal type, select Enable budget appropriation on the General ledger parameters page. The budget journal entries include information based on the ledger accounts defined on the Posting definitions page.

Check/Payment reversal:

You can use the Check/Payment reversal journal type to reverse a posted check. To use this journal type, select Use review process for payment reversals on the Cash and bank management parameters page.

Customer payment journal:

You can create customer payment transactions by using this journal. You use it to settle receivables.

Deposit slip payment cancellation:

You can cancel a deposit slip by using the Deposit slip payment cancellation journal. To use this journal type, select Use review process for deposit slip payment cancellations on the Cash and bank management parameters page.

Elimination journal:

You can create elimination transactions in an eliminations journal. To use this journal type, select Use for financial elimination process and Use for financial consolidation process on the Legal entities page. Before you can use this journal type, you must create a ledger elimination rule on the Ledger elimination rule page.

Fixed asset journal:

This journal can post fixed asset transactions.

General journal:

This journal is used to post financial transactions to general ledger accounts and other accounts, such as bank, customer, and vendor accounts. Posting with a general journal always creates entries on general ledger accounts. This is true even when a user posts a journal line to a customer account, because an entry is posted to a general ledger receivables account through a posting group.

Global General journal:

This is a newly introduced journal in Finance. You can use it to move between legal entities without switching the legal entity. It increases the productivity of general ledger accountants who work across legal entities.

Invoice approval journal:

You can post approved vendor invoices to the appropriate ledger accounts.

Invoice register:

This journal can register basic information about vendor invoices.

Periodic journal:

This journal can create periodic transactions based on schedule.

Process allocation journal:

You can create an allocation transaction in an allocations journal. Before you can create an allocation journal, you must create an allocation rule on the Ledger allocation rule page.

Project expense Journal:

You can create project expense transactions by using this journal.

Remittance journal:

You can create a bill of exchange remittance file for a customer, which can be sent to your organization's bank by using this journal. You can also use this journal to create a promissory note remittance file for the vendor that can be sent to your organization's bank.

Reporting currency adjustment Journal:

You can make adjustments in the reporting currency for balances on ledger accounts by using this journal.

Vendor invoice pool:

This journal can create vendor invoice pool transactions.

Vendor payment journal:

This journal can create vendor disbursement transactions to settle accounts payable.

Using the general journal, we can also perform intercompany and/or cross-currency finance transactions.

**SUMMARY**

- **Introduction to General Ledger:** Dynamics 365 Finance is introduced as a tool for managing accounting processes, including classifying, sorting, storing, and summarizing financial transactions related to assets, liabilities, and capital.
- **Chart of Accounts:** Explains the concept of a chart of accounts (COA), which serves as an index of all financial accounts. It discusses configuring ledger and journal setups, including linking multiple ledgers to a single COA.
- **Financial Dimensions:** Describes different types of financial dimensions, including custom and entity-backed dimensions, and how they are set up. It emphasizes the importance of evaluating business processes when defining financial dimensions.
- **Periodic Financial Processes:** Covers the various tasks involved in closing financial periods, such as settling invoices, posting transactions, running currency revaluation, performing reconciliations, and generating financial statements.
- **Year-End 1099 Reporting:** Explains the requirement to track and report payments made to vendors subject to 1099 tax reporting in the United States. It outlines the process of tracking 1099 amounts throughout the year and generating tax statements.
- **Journaling Concepts:** Discusses the purpose of journal entries in recording business transactions and their role in the general ledger. It provides an overview of different types of financial journals available in Dynamics 365 Finance, including budget journals, customer payment journals, and more.

MULTIPLE CHOICE QUESTIONS (MCQ) FOR PRACTICE

- 1 What is the primary function of Dynamics 365 Finance?
 - a) Inventory management
 - b) Financial management
 - c) Customer relationship management
 - d) Human resource management

- 2 What is a chart of accounts (COA) in Dynamics 365 Finance?
 - a) A list of customers
 - b) A list of financial transactions
 - c) An index of financial accounts
 - d) A list of employees

- 3 How can multiple ledgers be linked to the same chart of accounts in Dynamics 365 Finance?
 - a) It is not possible to link multiple ledgers to the same COA.
 - b) By configuring ledger rules
 - c) By creating custom dimensions
 - d) By using different financial systems

- 4 What are financial dimensions used for in Dynamics 365 Finance?
 - a) Managing inventory
 - b) Generating reports
 - c) Classifying financial transactions
 - d) Tracking employee data

- 5 Which of the following is NOT a type of financial dimension in Dynamics 365 Finance?
 - a) Custom dimensions
 - b) Entity-backed dimensions
 - c) Vendor dimensions
 - d) Sales dimensions

- 6 When might you create custom financial dimensions in Dynamics 365 Finance?
 - a) To represent legal entities
 - b) To track inventory
 - c) To report sales tax
 - d) To manage employee data

- 7 What is the purpose of the periodic financial closing process?
 - a) To open new financial periods
 - b) To generate annual financial statements
 - c) To settle invoices
 - d) To calculate tax liabilities

- 8 In Dynamics 365 Finance, what does the term "year-end 1099 reporting" refer to?
- a) Reporting financial transactions at the end of each month
 - b) Reporting income tax returns
 - c) Reporting payments to vendors subject to tax reporting
 - d) Reporting annual budget allocations
- 9 What is the primary purpose of a journal entry in accounting?
- a) Generating invoices
 - b) Recording business transactions
 - c) Calculating payroll
 - d) Managing customer relationships
- 10 Which of the following is NOT a type of financial journal in Dynamics 365 Finance?
- a) Budget journal
 - b) Customer payment journal
 - c) Sales order journal
 - d) Invoice register
- 11 What is the function of the "Global General journal" in Dynamics 365 Finance?
- a) To create fixed asset transactions
 - b) To consolidate financial data across companies
 - c) To generate financial statements
 - d) To manage customer payments
- 12 Which journal type is used to settle receivables in Dynamics 365 Finance?
- a) Invoice register
 - b) Periodic journal
 - c) Customer payment journal
 - d) Vendor payment journal
- 13 When does Dynamics 365 Finance typically generate an "Opening transaction" during the year-end close process?
- a) To close the fiscal year
 - b) To create the opening balances in the new fiscal year
 - c) To eliminate transactions
 - d) To process payroll
- 14 What is the purpose of the "Remittance journal" in Dynamics 365 Finance?
- a) To generate financial statements
 - b) To create vendor disbursement transactions
 - c) To manage fixed assets
 - d) To create year-end tax reports

- 15 In Dynamics 365 Finance, what are elimination transactions used for?
- a) Eliminating unnecessary financial records
 - b) Removing transactions between parent and subsidiary companies
 - c) Creating financial statements
 - d) Managing payroll

Answers

- 1 *b. Financial management*
- 2 *c. An index of financial accounts*
- 3 *b. By configuring ledger rules*
- 4 *c. Classifying financial transactions*
- 5 *c. Vendor dimensions*
- 6 *a. To represent legal entities*
- 7 *b. To generate annual financial statements*
- 8 *c. Reporting payments to vendors subject to tax reporting*
- 9 *b. Recording business transactions*
- 10 *c. Sales order journal*
- 11 *b. To consolidate financial data across companies*
- 12 *c. Customer payment journal*
- 13 *b. To create the opening balances in the new fiscal year*
- 14 *b. To create vendor disbursement transactions*
- 15 *b. Removing transactions between parent and subsidiary companies*

**SELF-EXAMINATION QUESTIONS FOR PRACTICE:**

- 1 What is the primary purpose of Dynamics 365 Finance in managing financial transactions for a company?
- 2 Explain the concept of a chart of accounts (COA) and its significance in financial management.
- 3 How does Dynamics 365 Finance allow the linking of multiple ledgers to a single chart of accounts?
- 4 What is the role of financial dimensions in Dynamics 365 Finance, and what are the two main types of financial dimensions discussed?
- 5 In what scenarios would you consider creating custom financial dimensions, and what are some potential limitations to this approach?
- 6 Describe the key tasks involved in the periodic financial closing process as outlined in the content.
- 7 What is the significance of year-end 1099 reporting in Dynamics 365 Finance, and which types of payments are typically subject to this reporting?
- 8 What are journal entries, and why are they important in accounting and financial management?
- 9 Provide examples of different types of financial journals available in Dynamics 365 Finance and their respective purposes.
- 10 How does Dynamics 365 Finance support intercompany and cross-currency finance transactions through the general journal?

CHAPTER 5

DESCRIBE ACCOUNTS PAYABLE AND ACCOUNTS RECEIVABLE IN DYNAMICS 365 FINANCE



LEARNING OBJECTIVES

- Describe core accounts payable components, including vendors, purchase orders, and vendor invoices.
- Describe vendor payments and settlements, including three-way matching concepts.
- Describe core accounts receivable components, including customers, customer invoices, and free text invoices.
- Describe credit and collection processes.
- Describe revenue recognition.

5.1. INTRODUCTION

Finance allows you to manage the accounting processes involved in paying vendors or suppliers for goods or services received and receiving payments for goods or services delivered.

In this module, you explore core accounts payable components, such as vendor invoices and purchase orders, and learn how to handle vendor payments. You also discover core accounts receivable processes, such as customers, customer invoices, and free text invoices. Finally, you explore credit and collection processes, such as credit management and collections management.

5.2. DESCRIBE CORE ACCOUNTS PAYABLE COMPONENTS

Accounts payable is money owed to suppliers presented as a liability on a company's balance sheet as short-term debt. For example, a restaurant might receive a shipment of food before the food is paid for. This debt is part of its trade payables.

Vendors:

A company purchases goods and services from vendors. Each accounts payable transaction must be associated with a vendor. Use the Vendors page to create, maintain, and inquire about vendors.

Always enter as much data as possible when you set up a new vendor in Finance, because that data is used throughout the system for invoices, payments, and reports.

The base data automatically appears as the default for all transactions involving the vendor, but default information can always be changed if you need to override it.

Vendor invoices:

To understand vendor invoices, you must first examine where they fit in with the business processes for Accounts payable, as presented in the following illustration:

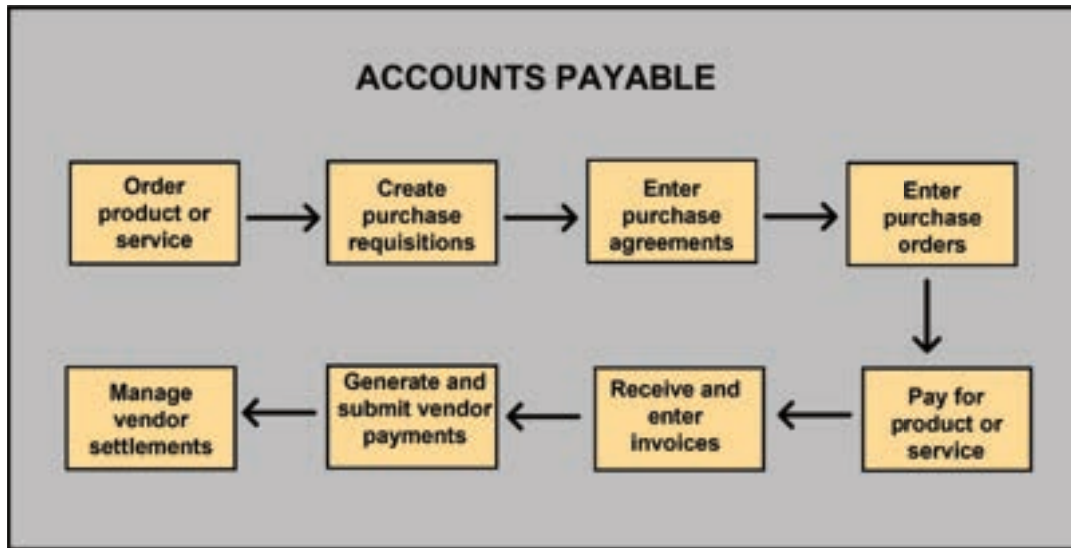


Figure 5.1. The Accounts payable business processes

When ordering a product or service from a vendor, you need to create purchase requisitions, enter purchase agreements, and enter purchase orders. Then, as a part of Accounts payable, you'll need to pay for the product or service. This involves receiving and entering invoices, generating and submitting vendor payments, and managing vendor settlements.

You can enter vendor invoices manually or receive them electronically through a data entity. When creating an invoice, you can also attach an electronic copy of the invoice to the record. After the invoices are entered or received, you can review and approve the invoices by using an invoice approval journal or the Vendor invoice page. You can use invoice matching, vendor invoice policies, and workflow to automate the review process so invoices that meet certain criteria are automatically approved, and the remaining invoices are flagged for review by an authorized user.

A vendor invoice from a purchase order is produced when products or services are received according to a purchase order placed with a vendor. The vendor invoice contains a header and one or more lines for items or services. A vendor invoice completes the cycle from purchase order to product receipt to vendor invoice.

Although some vendor invoices connect to a purchase order, vendor invoices can also contain lines that don't correspond to purchase order lines. You can also create vendor invoices that aren't associated with any purchase order. These vendor invoices might represent ongoing services, such as a utility bill. You don't have to reference a purchase order when you add an ongoing service.

You can enter a vendor invoice in several ways:

- The vendor invoice register lets you quickly enter invoices that don't reference a purchase order so you can accrue the expense. By using the vendor invoice approval journal, you can select those invoices and post them to the vendor balance to reverse the accrual.
- In a single step, the vendor invoice journal lets you quickly enter invoices that don't reference a purchase order.
- Together with the vendor invoice pool, the vendor invoice register lets you quickly enter invoices to accrue the expense. You can open the associated purchase orders later to post the invoice against the expense account.
- The Open vendor invoices and Pending vendor invoices pages let you create vendor invoices from confirmed purchase orders.

Purchase order:

A purchase order is a document that represents an agreement with a vendor to buy goods or services. The document also helps keep track of product receipts made toward the order and, later, the accounting of vendor invoices that the vendor bills toward the order.

The Purchase orders page contains an overview of the available orders and lets you modify those orders. When you open a purchase order, you can select the Header view, which contains information that is specified only one time for each purchase order, such as the vendor details. Alternatively, you can select the Lines view, where you can modify order lines. Typically, you'll switch between these two views as you modify purchase order. Charges aren't listed directly on the Purchase orders page, but they're accessed via menus on the order header and lines.

There are many reports where you can view information about purchase orders, product receipts, and vendor invoices. These reports are found in the Procurement and sourcing and Accounts payable modules.

The Purchase order preparation and Purchase order receipt and follow-up workspaces let you view lists of purchase orders in the various states that they have progressed to. They also provide a summary of the actions that must be taken. The Purchase order preparation workspace is focused on purchase order creation and review, order processing through approval, and confirmation with the vendor. The Purchase order receipt and follow-up workspace is focused on processing the receipt of goods or services against purchase orders. It includes lists that give insight into receipts that are overdue or that will soon be due for delivery by the supplier. These workspaces aren't used to perform the related receipt activities done in the warehouse. Those activities are performed by using pages in the Inventory management and Warehouse management modules. Processing vendor invoices should be done by using the Vendor invoice entry workspace, and payments should be done by using the Vendor payments workspace.

Three-way matching policies:

A “three-way match” refers to the three components (purchase order, receipt of goods, and supplier invoice) that must match within agreed-upon tolerance levels to ensure a proper and timely payment.

Let's examine a three-way matching example for item and vendor combination.

Summary: A controller at the corporate headquarters of a legal entity named Fabrikam decides that all invoices based on purchase orders should be matched with purchase order lines (two-way matching). The bookkeeper at the Malaysia division of Fabrikam can override the matching policy to a higher level of matching for specific purchase orders.

The volume and amounts are small, and there have been problems with delivery from some vendors in Malaysia. For these reasons, the bookkeeper sets the level of control for certain item and vendor combinations procured in Malaysia to three-way matching.

The invoice matching policies in this example help people in the following roles meet these goals:

- The controller for the Fabrikam enterprise can help the people in their organization identify and correct problems with ordering, receiving, and paying for items (goods and services) from vendors.
- The bookkeeper for the Malaysia division of Fabrikam can enforce corporate policy and make sure invoices are paid only after they're matched with purchase order lines and product receipts that represent the receipt of goods and services. The bookkeeper can also increase the level of control to three-way matching for specific items to control operational costs.

Prerequisites:

- The controller sets the matching policy at the legal entity level to Two-way matching.
- The controller sets the Match price totals field for the legal entity to Percentage and enters 10% as the tolerance percentage.
- The controller sets the unit price tolerance for all items to 2%.
- The bookkeeper sets the matching policy at the item and vendor combination level for item PH2500 – Computer and vendor Contoso to Three-way matching.
- A purchase order clerk at the Malaysia division of Fabrikam, issues purchase orders to Contoso to supply three items, as depicted in the following table. When they create the purchase order, they override the matching policy for the wireless mouse to be three-way matching instead of two-way matching.

Item number	Quantity	Unit price	Net amount	Matching policy (default entry)	Matching policy (on the purchase order line)
PH2500 – Computer	2	2,500.00	5,000.00	Three-way matching	Three-way matching
MM01 – Wireless Mouse	2	40.00	80.00	Two-way matching	Three-way matching
USB Drive	200	10.00	2,000.00	Two-way matching	Two-way matching

Scenario:

- The items arrive. A worker in the receiving department of the Malaysia division of Fabrikam is interrupted and doesn't post the product receipt immediately.
- The accounts payable coordinator at Fabrikam enters and verifies the invoice submitted by Contoso. They verify the following information:
 - o For items that require three-way matching, the quantity on the invoice line matches the quantity that was received. The received quantity is indicated on the product receipt that is matched to the invoice.
 - o For items that require two-way or three-way matching, the prices on the invoice line are within the tolerances defined in the application. This includes the following types of price matching:
 - Net unit price matching – The net unit price on the invoice line matches the net unit price on the purchase order line, within the tolerance percentage. In this example, the net unit price tolerance is +2%.
 - Price totals matching – The net amount on the invoice line matches the net amount on the purchase order line, within the tolerance percentage, amount, or percentage and amount. In this example, the price totals matching tolerance is +10%.

The paper invoice from Contoso contains the following information:

Item	Quantity	Unit price	Net amount
PH2500 – Computer	2	2,500.00	5,000.00
MM01 – Wireless Mouse	2	41.00	82.00
USB Drive	200	10.05	2,010.00
Total invoice			7,092.00

The invoice line includes the following information.

Item number	Quantity	Unit price	Line net amount	Matching policy	Product receipt quantity match	Price match	Price total match
PH2500 – Computer	2	2,500.00	5,000.00	Three-way matching	Failed	Passed	Passed
MM01 – Wireless Mouse	2	41.00	82.00	Three-way matching	Failed	Failed	Passed
USB Drive	200	10.05	2010.00	Two-way matching		Passed	Passed

Note:

For the PH2500 – Computer line, the Product receipt quantity match column has a warning icon, because the invoice line isn't matched to a product receipt. For the MM01 – Wireless Mouse line, the Product receipt quantity match column has a warning icon, because the invoice line isn't matched to a product receipt. The Unit price match column has a warning icon, because the 2% net unit price tolerance is exceeded. For the USB Drive line, the Product receipt quantity match

column is blank, because two-way matching doesn't match invoice line and product receipt line quantities.

If approval is required for invoices to be posted with invoice matching discrepancies, the Approve posting with matching discrepancies toggle on the Invoice matching details page must be selected before the invoice can be posted with price matching errors and quantity matching errors. If approval isn't required, invoice processing can continue if there are no other posting errors.

5.3. DESCRIBE VENDOR PAYMENTS AND SETTLEMENTS

When paying for a product or service ordered from a vendor, you need to receive and enter invoices, generate and submit vendor payments, and manage vendor settlements.

There are multiple methods to enter a vendor payment, including using a payment proposal, manually entering a one-off payment, and prepayments. You'll manage them from Accounts payable > Payments > Payment journal.

Create vendor payments by using a payment proposal:

Payment proposals are often used to create vendor payments, because the query can be used to quickly select vendor invoices for payment based on criteria such as the due date and cash discount.

Organizations often use payment proposals to create vendor payments, because the payment proposal query can be used to quickly select vendor invoices for payment based on the due date, cash discount, and other criteria.

Let's review an example. Fabrikam works with vendors who have issued the invoices in the following table:

Vendor	Invoice	Invoice date	Invoice amount	Due date	Cash discount date	Cash discount amount
3050	1001	June 15	500.00	July 15	June 29	10.00
3050	1002	June 20	600.00	July 20	July 4	12.00
3075	1003	June 15	250.00	June 28		0.00
3100	1004	June 17	100.00	July 17	July 1	1.00

On July 1, the accountant who handles payments at Fabrikam, pays vendors. The accountant uses a payment proposal to help complete this task more efficiently.

Option 1: By cash discount

The accountant selects Cash discount as the proposal type. They enter a date range of June 26 to July 10. The following invoices are included in the proposal:

- 1002, because the discount date of July 4 is in the range of payment dates.
- 1004, because the discount date of July 1 is in the range of payment dates.

The following invoices aren't included in the proposal:

- 1001, because the discount date of June 29 has already expired, so this invoice is no longer eligible for the cash discount.
- 1003, because this invoice doesn't have a discount date.

Option 2: By due date

The accountant selects Per due date as the proposal type. They enter a date range of June 26 to July 10. The following invoice is included in the proposal:

- 1003, because the due date of June 29 is in the range of payment dates.

The following invoices aren't included in the proposal:

- 1001, because the due date of July 15 is outside the range of payment dates.
- 1002, because the due date of July 20 is outside the range of payment dates.
- 1004, because the due date of July 17 is outside the range of payment dates.

Option 3: By due date and cash discount

The accountant selects Due date and cash discount as the proposal type. They enter a date range of June 26 to July 10. The following invoices are included in the proposal:

- 1003, because the due date of June 29 is in the range of payment dates.
- 1002, because the discount date of July 4 is in the range of payment dates.
- 1004, because the discount date of July 1 is in the range of payment dates.

The following invoice isn't included in the proposal:

- 1001, because the discount date of June 29 has already expired, so this invoice is no longer eligible for the cash discount, and the due date of July 15 is also outside the date range.

Prepayments:

Organizations might issue prepayments (advance payments) to vendors for goods or services before those goods or services are fulfilled.

Two methods can be used to issue prepayments to vendors: prepayment invoicing and prepayment journal vouchers. To minimize risk, you can track prepayments by defining the

prepayment on a purchase order. For this method, you must create a prepayment invoice that is associated with a purchase order. This method is referred to as prepayment invoicing. Organizations that don't want to track prepayments as closely or don't receive a prepayment invoice from their vendor can use prepayment journal vouchers instead of the prepayment invoicing method. You can create prepayment journal vouchers by creating journal entries and marking them as prepayment journal vouchers. For this method, you can't track which prepayments to a vendor are made against which purchase orders. However, you can mark a posted prepayment for settlement against a purchase order.

Settlements:

Settlement is the process of applying payment to an invoice.

Now let's examine an example of settlement.

Settle a partial vendor payment and the final payment in full before the discount date.

In this scenario, partial payments are made for a vendor invoice, and a cash discount is taken.

Fabrikam buys goods from vendor 3064. The vendor gives Fabrikam a cash discount of 1 percent if the invoice is paid in 14 days. Invoices must be paid in 30 days. The vendor also lets Fabrikam take cash discounts on partial payments. The settlement parameters are located on the Accounts payable parameters page.

Vendor invoice on June 25:

On June 25, the accountant enters an invoice for 1,000.00 for vendor 3064. They can view this transaction on the Vendor transactions page.

From the Vendors page, the accountant opens the Settle transactions page. The accountant can use the Settle transactions page to view the dates and amounts of cash discounts. The due date is July 25, and a cash discount of -10.00 is available if the invoice is paid by July 9.

Partial payment on July 1 by using the Settle transactions page:

The accountant can create a payment journal for this payment by opening the Payment journal page in Accounts payable. They create a new journal and enter a line for vendor 3064. They then open the Settle transactions page to mark the invoice for settlement. The accountant marks the invoice and changes the value in the Amount to settle field to -500.00. They notice that the value in the Cash discount amount field is -10.00 for the full invoice and that the value in the Cash discount amount to take field is -5.05. Therefore, the accountant is settling -505.05 of this invoice.

Remaining amount paid on July 8:

The accountant pays the rest of the invoice for vendor 3064 on July 8, which is in the cash discount period. They create the payment journal on July 8 and mark the transaction for settlement. The accountant notices that the amount that must be settled is 495.00. The value in the Estimated cash discount field is -5.00, because the 5.00 discount was previously taken.

The accountant posts the payment journal and reviews the vendor transactions on the Vendor transactions page. The balance for the invoice is now 0.00.

Describe vendor payments:

Depending on the business requirements, different processes can be used for the vendor payment.



5.4. DESCRIBE CORE ACCOUNTS RECEIVABLE COMPONENTS

Accounts receivable is money owed to a business by its customers presented as an asset on a company's balance sheet. For example, an electric company that bills customers for electricity after the customer has already received it would record an account receivable until the customer pays.

Customers:

When customers buy products or services, you can create customer invoices based on sales orders or packing slips. You can also enter free text invoices that aren't related to sales orders. You can receive payments by using several different payment types. These include bills of exchange, cash, checks, credit cards, and electronic payments. If your organization includes multiple legal entities, you can use centralized payments to record payments in a single legal entity on behalf of the other legal entities.

Customer invoices

To discuss customer invoices, we must first examine where they fit in with the business processes for Accounts receivable, as depicted in the illustration:

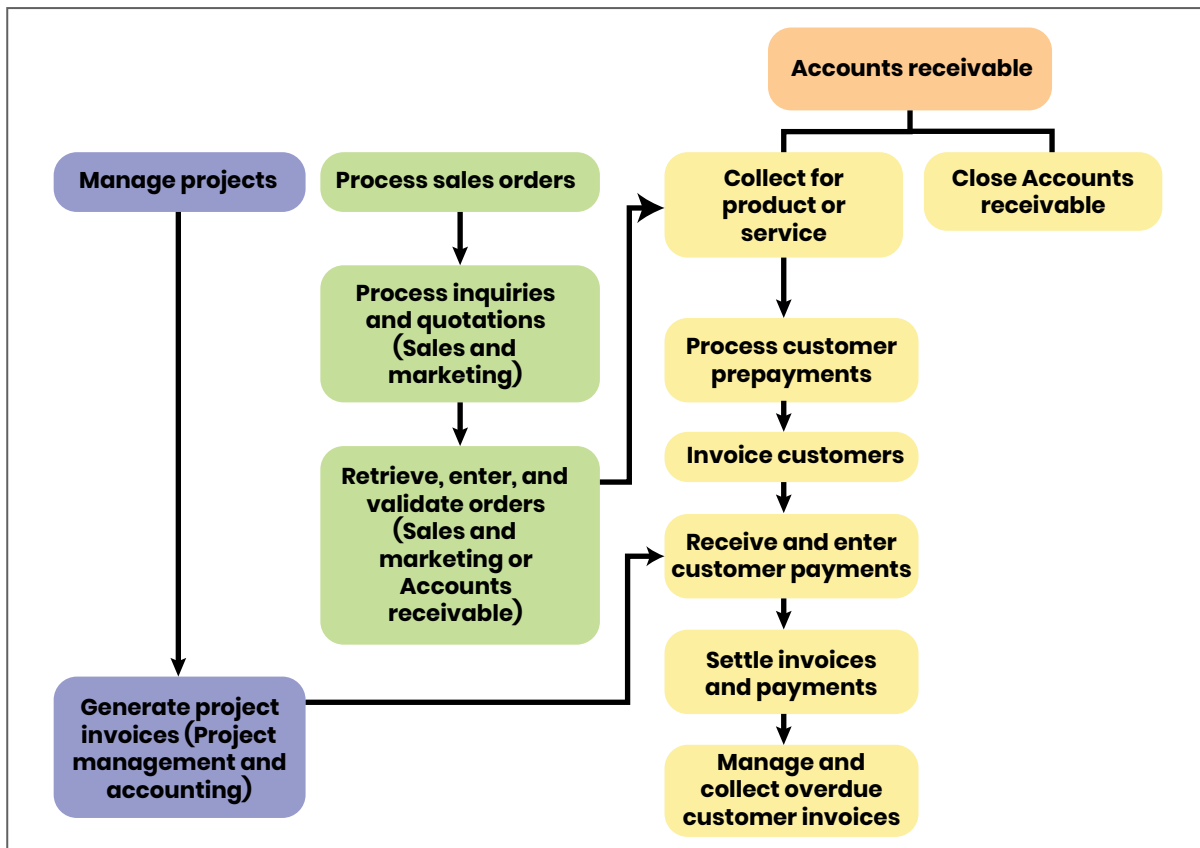


Figure 5.2. The Accounts receivable process and where Customer invoices fit in the process.

The Manage projects and Process sales orders processes feed into Accounts receivable in different steps of the Collect for product or service process. This process involves the following steps:

- Process customer prepayments.
- Invoice customers.
- Receive and enter customer payments.
- Settle invoices and payments.
- Manage and collect overdue customer invoices.

Three types of customer invoices are available:

- Customer invoices for sales orders
- Free text invoices
- Pro forma invoices

Customer invoices for sales orders:

A customer invoice for a sales order is a bill that is related to a sale and that an organization gives to a customer. This type of customer invoice is created based on a sales order, which includes order lines and item numbers. Item numbers are specified and posted in the ledger.

Free text invoices:

A free text invoice isn't related to a sales order. It contains order lines that include ledger accounts, free-text descriptions, and a sales amount that you enter. You can't enter an item number on this kind of invoice. You must enter the appropriate sales tax information. A main account for the sale is indicated on each invoice line, which you can distribute to multiple ledger accounts by selecting Distribute amounts on the Free text invoice page. Additionally, the customer balance is posted to the summary account from the posting profile used for the free text invoice.

Accounting distributions:

Accounting distributions are used to define how an amount will be accounted for, such as how the revenue, tax, or charges are accounted for on a free text invoice. Every amount that must be accounted for when the free text invoice is journalized will have one or more accounting distributions.

You can use the following buttons in the Free text invoice page to view, and possibly change, the accounting distributions for each amount on the free text invoice.

- Distribute amounts - View and change the accounting distributions for an individual line and any child lines, such as taxes or charges. You can also view and change the accounting distributions for the child line directly from the Sales tax transactions page or the Charges transactions page.

- o Change free text invoice header amounts, such as charges or currency rounding amounts.
 - o Change free text invoice line amounts.
- View distributions - View the accounting distributions for all lines on the document. You can't change the accounting distributions from this view.
 - o View header and line amounts.

Pro forma invoices:

A pro forma invoice is an invoice that is prepared as an estimate of the actual invoice amounts before the invoice is posted. You can print a pro forma invoice either for a customer invoice for a sales order or for a free text invoice.

5.5. DESCRIBE CREDIT AND COLLECTION PROCESSES**Credit management:**

Customer credit management lets you manage credit limits and control the flow of sales orders through the posting process based on credit rules you create.

The credit management process can include any of the following steps:

- Update credit attributes for customers to provide additional information about their credit worthiness.
- Create credit limits for customers by using credit limit adjustments.
- Create temporary credit limits for customers by using credit limit adjustments. In this way, you can temporarily increase or decrease customer credit limits based on business requirements.
- Add information that can affect the credit limit, such as information about insurance and guarantees.
- Create customer credit groups that link customers together so they share a single credit limit.
- Assign risk scores to customers, and then use the scores to automatically generate credit limits for those customers through credit limit adjustments.
- Create blocking rules that put an order on hold during one or more posting processes based on factors such as risk, payment terms, credit limits, overdue amounts, and the percentage of the credit limit that has been used.
- Manage a list of sales orders that are on hold, review the reasons for the hold, and mitigate issues.
- Release sales orders so they continue through the posting process.
- Set up a workflow to manage the approval of credit limit changes and sales order releases.

Collections management:

The Collections page provides a centralized view where accounts receivable collections information is managed. Collections managers can use this centralized view to manage collections. Collections agents can begin the collections process either from customer lists that are generated by using predefined collection criteria or from the Customers page.

Before you start to set up or work with collections, you should understand the following concepts:

- Customer aging snapshots contain aged balance information at a specific point in time.
- Collections customer pools help you organize your work.
- Collections agents can have their own customer pools.
- List pages organize collections customers, activities, and cases.
- All collections information for a customer is on one page, and you can take action from that page.
- Interest and fees can be waived, reinstated, or reversed in one step.
- Write-off transactions can be created in one step.
- Nonsufficient funds (NSF) payments can be processed in one step.

5.6. DESCRIBE REVENUE RECOGNITION

Revenue recognition is a financial process that involves the sale of a product, service, or subscription and breaks down the sales to multi-element lines. The revenue for these different lines is recognized according to the defined schedule based on the company-specific and industry-specific guidelines.

The revenue price, which is defined on the released products, can differ from the sale price. You can create a revenue schedule that determines the period for the revenue deferral. You can also define the revenue schedule on the sales order lines. The revenue price is calculated either when the sales order is confirmed or when the invoice is posted. To preview the revenue price before the invoice is posted, you must confirm the sales order. In the inventory posting profile, you can define the general ledger account to post the deferred revenue.

Revenue journal:

At the end of each period, you can create a revenue journal to release any scheduled lines that are due on or before a date they define. This revenue journal isn't posted immediately. Therefore, you can verify that the correct amounts are being released from deferred revenue to actual revenue.

The journal name needs to be created and set up under Revenue recognition > Setup > Journal names, with a company-specific number sequence for the voucher number. You also need to set up the default journal name under Revenue Recognition > Setup > General Ledger Parameters > Revenue recognition

Subscription billing:

The subscription billing feature is enabled from the Feature management workspace.

Subscription billing enables organizations to manage subscription revenue opportunities and recurring billing through billing schedules. Complex pricing, billing models, and revenue allocation are easily managed, billed, and recognized at the line level using this feature.

The feature has the following three modules that can be used independently or together.

- Recurring contract billing – This module enables recurring billing and price management to provide control over pricing and billing parameters, contract renewal, and consolidated invoicing.
- Revenue and expense deferrals – This module eliminates manual processes and dependency on external systems by managing revenue and enabling real-time insight into monthly recurring revenue.
- Multi-element revenue allocation – This module helps with revenue compliance by handling pricing and revenue allocation across multiple items.

The subscription billing feature can't be used with the revenue recognition feature. You must disable revenue recognition before enabling subscription billing.

SUMMARY**1 Accounts Payable and Accounts Receivable:**

Accounts payable involves managing the payment of vendors or suppliers for goods and services received.

Accounts receivable involves managing money owed to the company by customers for goods or services delivered.

2 Core Accounts Payable Components:

Vendors are entities from which a company purchases goods and services.

Vendor invoices can be generated manually or electronically and are linked to purchase orders.

Purchase orders are documents representing agreements with vendors for buying goods or services.

Three-way matching ensures the alignment of purchase orders, receipt of goods, and supplier invoices.

3 Vendor Payments and Settlements:

Vendor payments include processes like receiving and entering invoices, generating payments, and managing settlements.

Payment proposals are used to select vendor invoices for payment based on criteria like due date and cash discount.

Prepayments can be issued to vendors for goods or services in advance.

Settlement is the process of applying payments to vendor invoices.

4 Core Accounts Receivable Components:

Accounts receivable includes managing money owed to the company by customers.

Customer invoices can be based on sales orders, packing slips, or free-text descriptions.

Pro forma invoices provide estimates before the actual invoice is posted.

5 Credit and Collection Processes:

Credit management involves setting credit limits, creating customer credit groups, and managing sales order holds based on various factors.

Collections management provides a centralized view to manage collections, customer pools, agents, and more.

Various tools and workflows are used to streamline the credit and collections processes.

6 Revenue Recognition:

Revenue recognition involves breaking down sales into multi-element lines and recognizing revenue according to defined schedules.

Revenue price and schedule can be set at the product or sales order line level.

A revenue journal is used to release scheduled revenue at the end of each period.

Subscription billing is available as a feature to manage recurring revenue and billing.

7 Subscription Billing:

Subscription billing enables organizations to manage recurring billing, pricing, and revenue allocation.

It consists of three modules: recurring contract billing, revenue and expense deferrals, and multi-element revenue allocation.

Subscription billing and revenue recognition cannot be used simultaneously.

MULTIPLE CHOICE QUESTIONS (MCQ) FOR PRACTICE

- 1 What is the primary purpose of accounts payable in Dynamics 365 Finance?
 - a) To manage customer payments
 - b) To manage vendor payments
 - c) To track employee salaries
 - d) To record tax payments

- 2 What component is typically associated with a vendor transaction in Dynamics 365 Finance?
 - a) Sales Order
 - b) Purchase Order
 - c) Invoice Approval
 - d) Product Receipt

- 3 What is the main purpose of three-way matching in accounts payable?
 - a) To match vendor invoices with purchase orders and payments
 - b) To match vendor invoices with purchase orders and product receipts
 - c) To match vendor invoices with customer invoices
 - d) To match vendor invoices with sales orders

- 4 How can vendor invoices be entered in Dynamics 365 Finance?
 - a) Only through manual data entry
 - b) Only through electronic data entities
 - c) Both manually and electronically
 - d) Only through vendor invoice pools

- 5 What are purchase orders used for in the accounts payable process?
 - a) To request payment from customers
 - b) To record vendor expenses
 - c) To agree on the purchase of goods or services from vendors
 - d) To generate sales invoices

- 6 In Dynamics 365 Finance, what is the purpose of a payment proposal?
 - a) To settle customer invoices
 - b) To select vendor invoices for payment based on criteria
 - c) To create purchase orders
 - d) To generate sales orders

- 7 What is a pro forma invoice in accounts receivable?
 - a) An estimate of the actual invoice amounts before posting
 - b) An invoice generated based on sales orders
 - c) A finalized sales invoice
 - d) An invoice related to overdue payments

- 8 In accounts receivable, what is the purpose of credit management?
- a) To increase credit limits for all customers
 - b) To set credit limits and manage sales order holds
 - c) To eliminate all customer credit limits
 - d) To approve every sales order automatically
- 9 What is the primary function of collections management in Dynamics 365 Finance?
- a) To create purchase orders
 - b) To organize customer lists
 - c) To manage accounts receivable collections
 - d) To process vendor payments
- 10 What is revenue recognition in financial processes?
- a) The process of recognizing revenue from sales orders
 - b) The process of estimating future revenue
 - c) The process of breaking down sales into multi-element lines
 - d) The process of tracking vendor payments
- 11 Which module in Dynamics 365 Finance enables recurring billing and price management for subscriptions?
- a) Credit Management
 - b) Revenue Recognition
 - c) Subscription Billing
 - d) Collections Management
- 12 What is the purpose of a revenue journal in Dynamics 365 Finance?
- a) To record vendor payments
 - b) To release scheduled revenue to actual revenue
 - c) To manage customer credit limits
 - d) To create purchase orders
- 13 In Dynamics 365 Finance, what is the primary focus of the multi-element revenue allocation module?
- a) Managing credit limits for customers
 - b) Allocating revenue across multiple sales orders
 - c) Tracking vendor expenses
 - d) Creating purchase orders
- 14 Can subscription billing and revenue recognition features be used simultaneously in Dynamics 365 Finance?
- a) Yes
 - b) No

- 15 What financial aspect does accounts payable primarily deal with in Dynamics 365 Finance?
- a) Managing customer payments
 - b) Managing vendor payments
 - c) Tracking employee salaries
 - d) Recording tax payments

Answers

- 1 *B) To manage vendor payments*
- 2 *B) Purchase Order*
- 3 *B) To match vendor invoices with purchase orders and product receipts*
- 4 *C) Both manually and electronically*
- 5 *C) To agree on the purchase of goods or services from vendors*
- 6 *B) To select vendor invoices for payment based on criteria*
- 7 *A) An estimate of the actual invoice amounts before posting*
- 8 *B) To set credit limits and manage sales order holds*
- 9 *C) To manage accounts receivable collections*
- 10 *A) The process of recognizing revenue from sales orders*
- 11 *C) Subscription Billing*
- 12 *B) To release scheduled revenue to actual revenue*
- 13 *B) Allocating revenue across multiple sales orders*
- 14 *B) No*
- 15 *B) Managing vendor payments*

**SELF-EXAMINATION QUESTIONS FOR PRACTICE:**

- 1 What is the primary purpose of accounts payable and accounts receivable in Dynamics 365 Finance?
- 2 How can vendors be managed within the Dynamics 365 Finance system, and why is it important to input comprehensive vendor data?
- 3 Describe the typical process flow in accounts payable, including the steps from purchase order to vendor invoice approval.
- 4 What is three-way matching, and why is it essential in accounts payable processes?
- 5 Explain the various methods for entering vendor invoices in Dynamics 365 Finance.
- 6 What is the role of purchase orders in the accounts payable process, and how are they related to vendor invoices?
- 7 How can credit limits and customer credit groups be utilized in accounts receivable management?
- 8 Describe the different types of customer invoices available in Dynamics 365 Finance and their respective use cases.
- 9 What are the key steps involved in managing collections within Dynamics 365 Finance?
- 10 Can you explain the concept of revenue recognition and its significance in financial processes?

CHAPTER 6

EXPLORE EXPENSE MANAGEMENT, FIXED ASSET MANAGEMENT, AND BUDGETING IN DYNAMICS 365 FINANCE



LEARNING OBJECTIVES

- Describe cash and bank management concepts.
- Describe expense management, including cash advances.
- Describe fixed asset management and fixed asset creation, acquisition, and depreciation.
- Describe budgeting capabilities.

6.1. INTRODUCTION

With Finance, you can maintain your organization's bank accounts and the associated processes of managing expenses, tracking fixed assets, and balancing income and expenses for planning purposes.

In this module, you explore cash and bank management. You discover the core functionality of expense management and learn how to manage fixed assets. And finally, you review the budgeting capabilities of Finance.

6.2. DESCRIBE CASH AND BANK MANAGEMENT CONCEPTS

You can use the cash and bank management module to maintain the legal entity's bank accounts and the financial instruments associated with those bank accounts.

These instruments include deposit slips, checks, bills of exchange, and promissory notes. You can also reconcile bank statements and print bank data on standard reports.

The cash and bank management module is closely connected to the accounts receivable and accounts payable modules.

Business processes:

There are four major business processes under cash and bank management:

- Deposit bank funds.
- Reconcile bank accounts.
- Transfer bank funds.
- Manage letters of guarantee.

Deposit bank funds:

By using the cash and bank management module in Finance, you can maintain your legal entity's bank accounts and the financial instruments that are associated with those accounts. This might include deposit slips, bills of exchange, promissory notes, or checks.

A deposit slip is a document used to deposit checks, credit card notes, and cash into a bank account. Use the Deposit slip page to view and manage deposit slips for payments into bank accounts.

You can cancel a deposit slip payment if a customer payment is invalid. If you have already reconciled the deposit slip in the bank statement, you can't cancel the payment.

Reconcile a bank account:

When you receive a bank statement, you should periodically reconcile legal entity bank transactions with the transactions on the bank statement.

You can't reconcile a bank statement with a bank account if any of the checks or deposit slip payments listed on the statement currently have a status of Pending cancellation. After a reviewer posts or rejects a check reversal or deposit slip payment cancellation, the status is no longer Pending cancellation, and you can reconcile the bank account.

Manage letters of guarantee:

A letter of guarantee is an agreement by a bank (the guarantor) to pay a set amount of money to someone (the beneficiary) if a bank customer (the principal) defaults on a payment or an obligation to the beneficiary. Letters of guarantee aren't transferable. They apply only to the beneficiary who is named in the agreement. The principal can request an increase or decrease in the value of a letter of guarantee, subject to the terms of the agreement.

You can use the Letter of guarantee page to complete these tasks:

- Create correct ledger entries and eliminate manual entry.
- Record all monetary and nonmonetary transactions, and track balances of letters of guarantee.
- Record and track the status and expiration of letters of guarantee.
- Generate a report that lists the banks that are holding letters of guarantee.

Settlements:

During settlement, the transactions on one document are applied to the transactions on

another document to increase or decrease the balance of each document. For example, a payment can be applied to an invoice. Various types of transactions can be settled at different times through different methods. The settlement process can also generate new transactions.

Settlement can occur between any transaction types that affect the vendor balance or customer balance. These transaction types can include invoices, payments, credit memos, and fees. Any transaction type can be settled against any other transaction type.

The following transaction types are available for use in single-company and cross-company settlements:

- Settlement
- Cash discount
- Foreign currency revaluations (includes realized and unrealized foreign currency revaluations)
- Penny difference
- Overpayment/underpayment

6.3. DESCRIBE EXPENSE MANAGEMENT

In this unit, you'll learn about the core functionality of expense management, its streamlined features, and considerations for planning your implementation to enhance your organization's expense management capabilities.

Expense management capabilities are streamlined for your organization's expense management processes. You can use expense management to create automated workflows to collect payment method information and to be able to track how often the company credit card is used versus cash, for example. You can also import credit card purchases and monitor the money employees spend on your organization's expenses. You can use the expense policies and other out-of-the-box parameters to set up and manage Organization expenditures across categories and automate travel expense reimbursement.

In the Feature management workspace, you can enable the Expense reports reimaged feature to simplify the experience and reduce the time needed to complete expense reports. To customize the form fields' visibility, you can add a new Setup page and decide which data is required, optional, or unnecessary when expense reports are entered. When this feature is enabled, a new workspace for expenses opens.

The Expense management workspace is the landing page for creating and submitting expense reports. The screenshot depicts an example expense report:

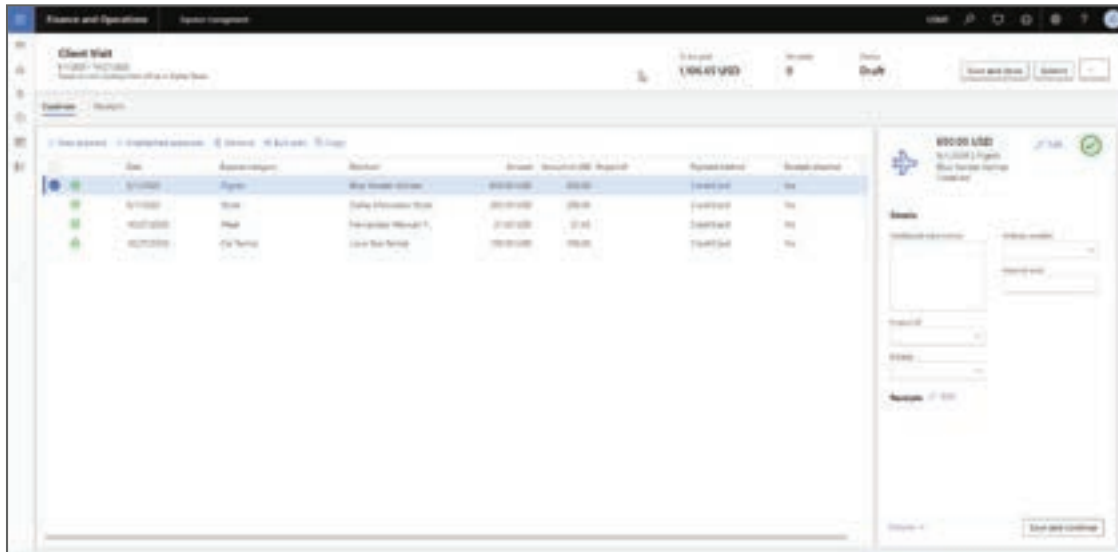


Figure 6.1. Expense management page.

Other features of expense reports include:

- Space for tracking expenditures that helps you view your delegate's expenses.
- Matching experience with receipts to help display receipts at the header level and improve the method of adding receipts to expense lines.
- Modern read-only grid that allows you to display even more expense lines and more data columns. Itemized and broken lines, along with their parental expenses, will appear.
- Streamlined expense editing pane.

The Expense reports reimagined feature gives you access to delegates' expenses through a modern Expense management workspace. It includes a simple and intuitive pane for editing expenses and an advanced error, warning, and policy messaging system. This messaging system ensures less downtime due to correcting or waiting for edits to submit an expense report successfully. If issues arise, the expense workflow can guide users to the error and offer suggestions on what to fix.

Expense management also offers gentle policy reminders to users to help the organization stay in compliance. To ensure that you're getting the full experience, make sure you use the Feature management workspace to enable the expense reports receipt matching feature.

Plan expense management:

An organization must make decisions and act when setting up Expense management during the planning period before deployment.

You can store details regarding payment methods, required travel requisitions, expense reports, rules, and so on, in Expense management. All choices that you make during the configuration of

cost management are based on the organization's hierarchy and financial background. Therefore, you must refer to the proper documentation for those areas of concern, such as specific tax rules for your organization or the location of the organization. These items could have specific rules and regulations that would need to be accounted for during the planning period.

Per diems:

The employee per diem provided by your company must be specified. Because per diems are typically used to cover expenses such as meals, accommodation, and other incidental expenses, you can build guidelines that your company provides for per diem allowances. The per diem might depend on the time of year, the travel destination, or both.

When you consider a per diem clause, you can specify that a portion of the per diem rate is withheld if a worker receives free meals or services. You can also determine per diem rate thresholds and set the minimum and the maximum number of hours that are added to a worker's travel by the per diem rate. The diagram depicts the per diem process:

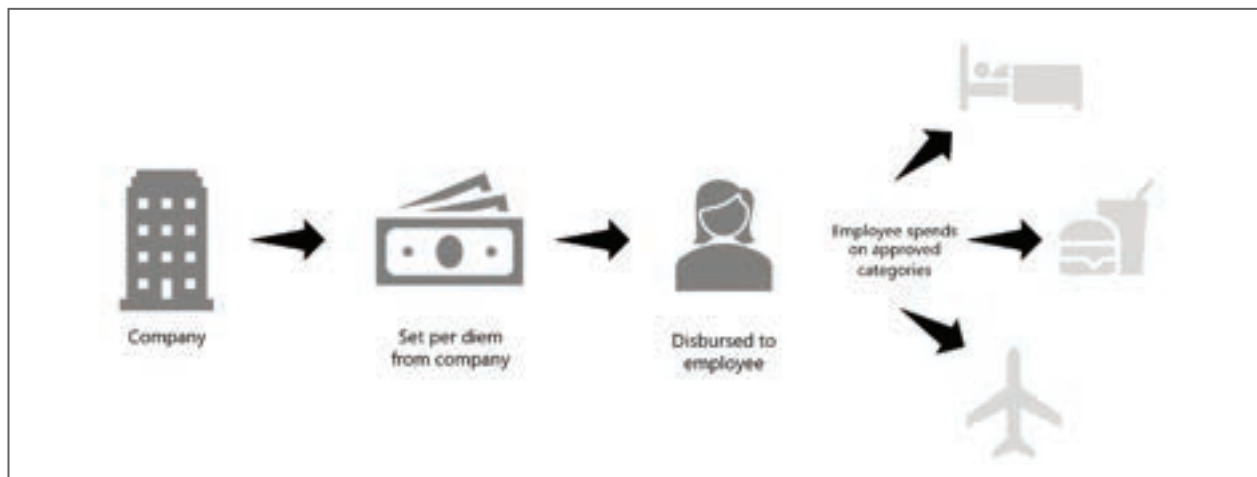


Figure 6.2.Per diem process.

Implement per diems:

You must make several decisions regarding the implementation of per diems. Ask yourself the following questions.

Default per diem rules for the first and last days:

- What is the minimum number of hours that an employee can claim for a day and still receive a per diem?
- Is there a reduction in the amount offered for meals, hotels, or other expenses for the first day and last day? If a reduction occurs, what is the percentage of the reduction?

Default per diem rules:

- Is a percentage reduction offered in the per diem allowance for each meal if, for example, the meal is complimentary? If a reduction is offered, what is the reduction percentage for each meal?
- Is the meal reduction calculated for each day, for each trip, or by the number of meals each day?
- Should per diem amounts be rounded in the regular manner or rounded up?
- Are per diems calculated on 24 hours or a workday?

The following screenshot depicts the parameter settings for the per diem configuration in the Expense management module.

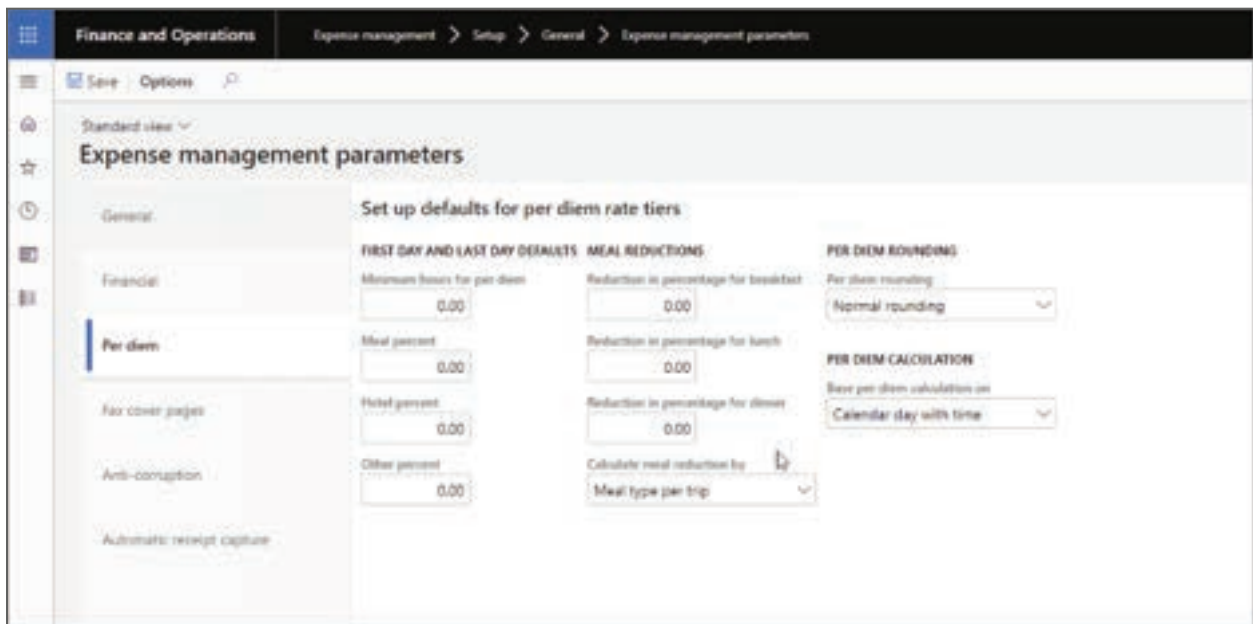


Figure 6.3. The Expense management parameters page where the Per diem tab is displayed.

Per diem rules that are based on location:

- Do per diem rates vary according to location? Which locations are included?
- If per diem rates vary according to location, for each location, what percentage amount is provided for the following types of expenses?
 - Meals
 - Hotel
 - Other expenses

Payment methods:

You must specify the payment methods employees are required to use when you allow them to incur expenses on behalf of your company. For instance, you might allow workers to use cash or

a corporate credit card. You could also allow employees to use personal credit cards and then reimburse them.

Policies:

Policies help guarantee that employees stay within budget, provide all required information, and spend money only as they need to.

Policy rules build into the expense categories the organization developed during the expense planning period. The screenshot depicts the Policy organizations page:

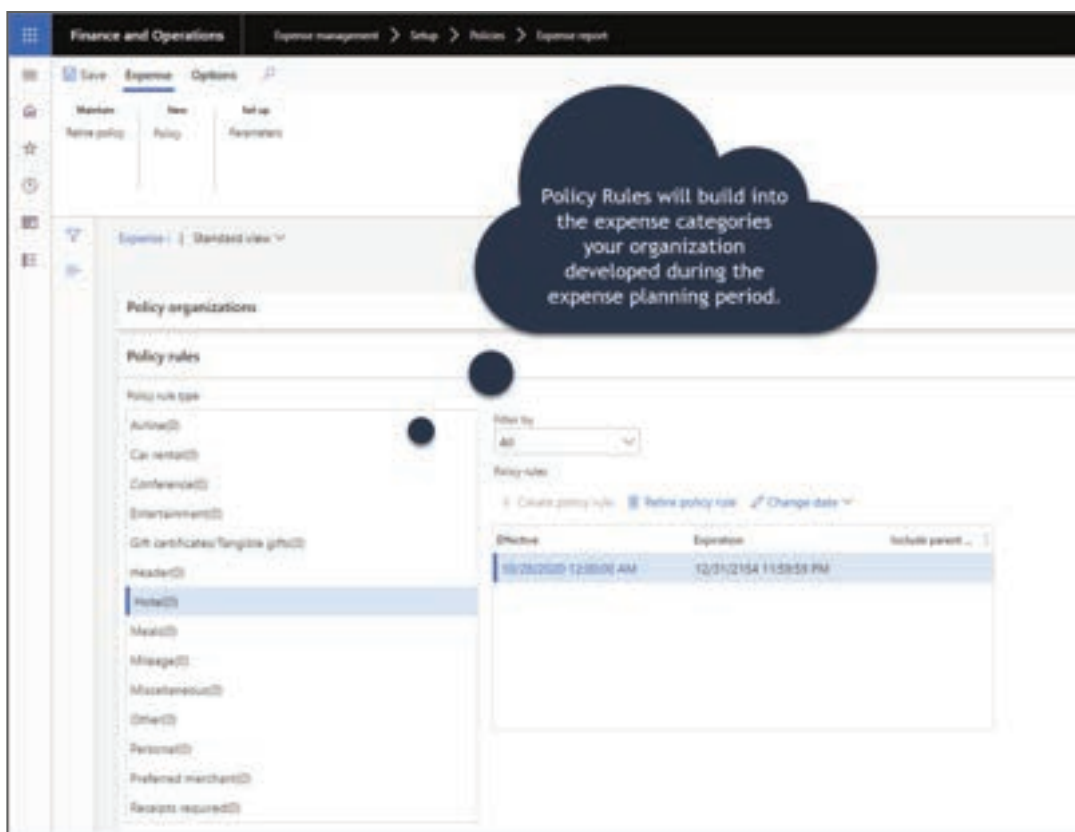


Figure 6.4. The Policy organizations page, which shows the different policy rules. The Hotel option is selected.

Note:

The expense categories can be shared between Project and Expense, or Project and Production, but not between Expense and Production.

Some widely used expense categories, depicted in the screenshot, include airfare, lodging, meals, and ground transportation.

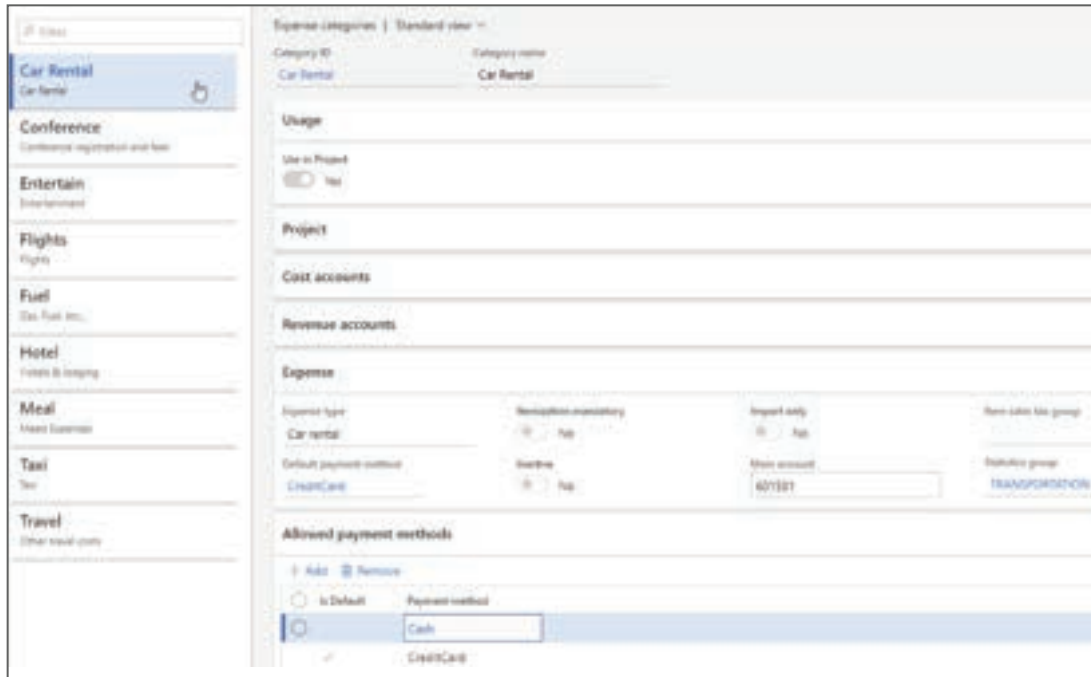


Figure 6.5.Screenshot depicts the different expense categories.

Consider the following questions when you establish expense categories for an organization:

- What is the type of expense? Categories for flights, hotels, or mileage are examples.
- Can the expense category also be used in Project management and accounting?
- Which default payment method should be selected for the expense category?
- Which account is the default for the expense category?

Next, let's explore fixed asset management.

6.4. DESCRIBE FIXED ASSET MANAGEMENT

Fixed assets and current assets:

In a company's balance sheet, assets are divided into two groups:

- Fixed assets
- Current assets

It's important to define the differences between fixed and current assets before discussing how to account for each. The classification of assets isn't based on the physical nature of the asset, but rather on the purpose of the asset ownership.

Current assets are those that a company depletes in the typical course of business over the next year or business cycle, whichever is shorter.

Examples of current assets include:

- Cash
- Accounts receivable
- Prepaid expenses
- Inventory

Fixed assets are assets that a company owns and uses in the daily operations of the company and aren't intended for resale to customers. The useful lives of these assets span multiple years.

Examples of fixed assets include:

- Vehicles
- Computers
- Machinery
- Buildings
- Copyrights or trademarks (a special class of assets frequently called intangible assets)

Based on these definitions, the same asset might be classified as a fixed asset in one company and as a current asset or inventory item in another.

An example of a company where the same asset might be classified as both fixed and current is an automobile dealership. The vehicles held for sale are inventory items in addition to current assets, whereas an employee's company car is a fixed asset.

Accounting for fixed assets:

All fixed assets are treated as balance sheet transactions in the year they're acquired, and they're posted as an asset to a balance sheet account.

Fixed assets represent permanent value and not just expenditures in the year of acquisition. They're typically depreciated, or expensed, over their useful life. Other adjustments might also be necessary. The most common transaction, known as depreciation, is an entry that expenses the part of the asset's original purchase price that was used during the year.

Various methods are used for depreciation. One of the methods, straight line, is computed by taking the costs of the acquisition and dividing those costs by the expected service life of the asset. The rules that determine the calculation of depreciation are defined in local legislation.

The screenshot depicts a list of fixed assets:

Fixed asset number	Name	Fixed asset group	Type	Location	Responsible
BUIL-000001	Corporate headquarters	BUILDINGS	Land and buildings	HQ	Ted Howard
BUIL-000002	Production Site 1	BUILDINGS	Land and buildings	PROD_1ST_F	Ted Howard
BUIL-000003	Warehouse Site 1	BUILDINGS	Land and buildings	WHOUSE_1ST	Pierre Hezi
BUIL-000004	Production Site 2	BUILDINGS	Land and buildings	PROD_2ND_F	Elen Gasca
BUIL-000005	Warehouse Site 2	BUILDINGS	Land and buildings	WHOUSE_2ND	Inga Namaduri
BUIL-000006	Production Site 3	BUILDINGS	Land and buildings	PROD_3RD_F	Lars Gæstl
BUIL-000007	Warehouse Site 3	BUILDINGS	Land and buildings	WHOUSE_3RD	Pierre Hezi
COMP-000001	Notebook PC	COMP	Tangible	HQ_1ST_FL	Tim Litton
COMP-000002	USB peripheral switch	COMP	Tangible	HQ	Tim Litton
COMP-000003	LCD monitor	COMP	Tangible	HQ_1ST_FL	Tim Litton
COMP-000004	Desktop PC	COMP	Tangible	HQ_2ND_FL	Tim Litton

Figure 6.6. List of fixed assets.

For all assets, the value of the asset in the balance sheet (net book value) should be reviewed at least once each year. You can do this monthly, quarterly, semi-annually, or annually. Together with this value review, an adjustment of the asset value in the balance sheet (write-down or write-up) might be necessary.

The write-down or write-up amounts are usually caused by some extraordinary occurrences in the market that affect the price if the company were to reacquire the asset. For example, the increased price of a building might be caused by the real estate market. Accounting principles in some countries or regions prohibit asset write-up.

When a company no longer has use for the asset, because it's either being sold or scrapped, the asset must be removed from the accounting books. Therefore, the original acquisition price and accumulated depreciation of the asset are reversed, and any surplus or loss from the disposal is posted to the profit and loss statement.

Relationships between fixed assets components:

The following diagram illustrates the relationships of the Fixed assets module in Finance.



Figure 6.7. An overview of fixed assets components.

Fixed asset groups let you group your assets and specify default attributes for every asset assigned to a group.

Books are assigned to fixed asset groups. Books track the financial value of a fixed asset over time by using the depreciation configuration defined in the depreciation profile.

You should first set up depreciation profiles. In the depreciation profile, you can configure how the value of an asset is depreciated over time. You need to define the method of depreciation, the depreciation year (calendar year or fiscal year), and the frequency of depreciation.

After you set up books, you can create the posting profile. The posting profile must be defined by book, but it can also be defined at a more detailed level. For example, you can define the posting profile for the combination of a book and a fixed asset group, or even for an individual fixed asset book. By default, the ledger accounts that are defined are used for your fixed asset transactions.

6.5. DESCRIBE BUDGETING CAPABILITIES

Plan basic budgeting:

When using basic budgeting in Finance, you need to compile information about how the budgets should be configured before you begin the configuration.

Before you begin configuring basic budgeting or budget control, you should compile the following information:

- Gather information about which financial dimensions and main accounts are used for budgeting and that can have amounts transferred either to or from them. (Main accounts are optional but used by most.)
- Define currency exchange rates and what those exchange rates are.
- Set up budget codes for each budget type, and determine which code is the default budget code.
- Decide which budget register entries use workflows. You can assign workflows to budget codes. The budget register entries that are associated with a budget code that has an assigned workflow are automatically submitted to workflow.
- Provide the names of each budget model.
- Choose how the budget cycles will be set up.
- Determine the amounts that will be allocated across periods or to other financial dimension values.
- Select financial dimensions that have recurring amounts.
- Decide which budget models will be used in cash flow forecasts.

Plan budget control:

If you use budget control, compile the following information in addition to the information in the Plan basic budgeting topic:

- Financial dimensions that should be included in budget control rules.
- User groups that can post entries that exceed the remaining balance for a budget.
- Source documents and accounting journals that should be enabled for budget checking.
- Financial dimensions and accounts that must have a budget threshold and what that threshold is. A budget threshold is the level of budget usage at which you can prevent posting or display warnings. For example, if the threshold is 80, you can warn a user during ledger transaction entry that 80 percent of the budget for the selected account has been used.
- The formula for calculating the remaining balance of a budget. The budget fund's available calculation can be defined for each legal entity instead of always using the following calculation: Original budget - Actual expenses.
- The interval, such as monthly, quarterly, or yearly, used to determine whether the available budget balance is enough to cover transactions.

Budgeting tools:

Other planning and budgeting capabilities are available in Finance. The following budgets are integrated with ledger budgets.

Workforce budgets – Workforce budgeting includes detailed budget cost component planning for positions, compensation groups, and so on.

Fixed assets budgets – Based on fixed asset information, you can calculate planned depreciation and record other planned transactions related to fixed assets.

Project budgets – In the Projects module, you can create detailed project forecasts. The projects forecasts include details about the planned hours, expenses, fees, and items.

Inventory budget – In the inventory budget, you estimate the money or capital needed to purchase inventory. The inventory budget includes the sales forecasts, bottom-up budgeting, vendor analysis, and internal inventory controls.

Demand forecasting – Based on historical transaction data, you can estimate future inventory demand and create demand forecasts.

Budgeting methodologies:

Several methodologies are available for defining budgets in your organization.

Two of these are:

- Zero-based budgeting
- Historical budgeting

Zero-based budgeting:

Zero-based budgeting is a method of planning and decision-making that reverses the working process of traditional budgeting. In traditional incremental budgeting, departmental managers justify only increases over the previous year's budget and what has already been spent is automatically allowed.

Advantages of using zero-based budgeting include:

- Allocating resources efficiently because it's based on needs and benefits.
- Driving managers to find cost-effective ways to improve operations.
- Helping to detect inflated budgets.

Historical budgeting:

Historical budgeting, sometimes referred to as incremental budgeting, uses a budget prepared by using a previous period's budget or actual performance as a base, with incremental amounts added for the new budget period.

Advantages of historical budgeting include:

- The budget is stable, and change is gradual.
- Managers can operate their departments on a consistent basis.
- The system is relatively simple to operate and easy to understand.

Basic budgeting overview:

You can use basic budgeting to define the financial dimensions for budgets, create budget models, and set up and use budget register entries. You can also set up optional budgeting workflows to automate review of budget register entries, including budget transfers.

For example, if an approval is required for transferring a budget amount from one department to another, then workflow functionality helps to create an approval workflow. This unit explains the basic budgeting and control processes.

Multiple methods exist for creating budget register entries in Finance:

- Manually enter the document information on the Budget register entries page.
- Use a Microsoft Excel template that you can open by selecting the Open in Excel button on the Budget register entries page.
- Use the Budget Account Entries data entity in Data management to import budget register entries. You should consider using this method and turning on the Set based processing parameter when you need to import many budget account entries into the system.
- Use the Generate budget register entry periodic process if the company uses Budget planning functionality to prepare budget data.

Budget control overview:

Budget control in Finance helps you manage financial resources. Budget control is a method of ensuring that enough budget funds are available for planned or actual purchases. After setting up basic budgeting, you can set up budget control.

Budget control in Finance supports management of an organization's financial resources

through the chart of accounts, workflows, user groups, source documents and journals, configurable calculation of available funds, budget cycles, and thresholds. When controls are in place, an organization can plan, measure, manage, and forecast its financial resources throughout its fiscal year.

You can configure budget control according to several factors:

- Financial dimensions - Discover which financial dimensions must be used to report budget and actuals, and which financial dimensions are required to control budget. Determine whether specific dimension combinations or main accounts require attention. For example, you might need to verify whether requirements exist to track budget to actuals by cost center and program, or if travel expenses require special attention.
- Time - Determine which time frame (fiscal period, fiscal period to date, and so on) will be used to evaluate available budget funds.
- Source documents - Establish which source documents must be evaluated for budget control and whether the documents should be evaluated per line or per document.
- Funds available calculation - Determine if documents such as purchase requisitions (pre-encumbrances) and purchase orders (encumbrances) should be considered in the calculation of available funds. Evaluate whether documents that are in a draft state should be considered in the calculation.
- Override permission - Discover who has permission to exceed the available budget.

Budget control is fully integrated with Finance. Therefore, you can evaluate the available budget for planned purchases and actual purchases. Budget inquiries and reports are available; therefore, users can evaluate the budget throughout the budget cycle and can make any adjustments that are required in the form of budget revisions or transfers. A budget manager can also export the budget and actuals into Microsoft Excel to better analyze and forecast as required.

Let's consider the following scenario: A purchasing agent creates a purchase order that has multiple lines. The first three lines are entered. When the purchasing agent enters the fourth line, a message is displayed that the financial dimension value is over budget.

The purchasing agent isn't in a user group that is authorized to exceed the budget. The purchasing agent can complete the fourth line, enter more lines, and save the purchase order in a Draft state.

The purchasing agent then notifies a manager of the over-budget situation. The budget manager has the authority to exceed the budget funds available. The budget manager can open the purchase order and continue with the purchase order confirmation without changing any amounts or accounts.

Later, the budget manager performs a budget transfer to increase the available budget for the financial dimension value that was over budget.



SUMMARY

Expense Management:

- Manages bank accounts, deposits, and reconciliations.
- Streamlines expense reporting with automated workflows.
- Offers receipt matching and policy reminders for compliance.

Fixed Asset Management:

- Tracks long-term assets, handles depreciation, and ensures accurate balance sheet reporting.
- Emphasizes regular asset value reviews and disposal processes.

Budgeting Capabilities:

- Allows for defining financial dimensions, creating budget models, and using budget register entries.
- Offers budget control for monitoring available funds.
- Integrates with Finance for real-time budget evaluation.

MULTIPLE CHOICE QUESTIONS (MCQ) FOR PRACTICE

- 1 What is the primary function of the expense management module in Dynamics 365 Finance?
 - a) Managing customer accounts
 - b) Managing employee salaries
 - c) Managing bank accounts and expenses
 - d) Managing inventory levels
- 2 Which financial instruments are associated with bank accounts in Dynamics 365 Finance?
 - a) Invoices and purchase orders
 - b) Checks and bills of exchange
 - c) Sales orders and receipts
 - d) Inventory items and vendors
- 3 In the context of cash and bank management, what does reconciliation refer to?
 - a) Balancing income and expenses
 - b) Reviewing employee salaries
 - c) Matching bank transactions with bank statements
 - d) Managing letters of guarantee

- 4 What is the purpose of a deposit slip in Dynamics 365 Finance?
- a) To create invoices for customers
 - b) To record employee expenses
 - c) To deposit checks and cash into a bank account
 - d) To manage vendor payments
- 5 In Dynamics 365 Finance, when can you reconcile a bank statement with a bank account?
- a) Anytime, regardless of transaction status
 - b) Only if all checks are cleared
 - c) Only if there are no pending cancellations
 - d) Only after all expenses are approved
- 6 What is a letter of guarantee, and how is it managed in Dynamics 365 Finance?
- a) An agreement to pay a set amount if a customer defaults; managed in the Letter of guarantee page
 - b) A contract with a vendor; managed in the Vendor Contracts module
 - c) A type of expense report; managed in the Expense Management workspace
 - d) An agreement with a bank; managed in the Cash and Bank Management module
- 7 Which feature in Dynamics 365 Finance streamlines the expense reporting process by simplifying form fields and offering policy reminders?
- a) Budgeting capabilities
 - b) Expense reports reimaged
 - c) Fixed asset management
 - d) Cash and bank management
- 8 What should an organization consider during the planning phase before implementing expense management in Dynamics 365 Finance?
- a) Tax regulations for their location
 - b) Supplier negotiation strategies
 - c) Employee training programs
 - d) The organization's hierarchy and financial background
- 9 In Dynamics 365 Finance, what are per diems used for in expense management?
- a) Tracking employee attendance
 - b) Estimating inventory costs
 - c) Covering expenses such as meals and accommodation
 - d) Calculating depreciation for fixed assets

- 10 When implementing per diems in Dynamics 365 Finance, what factor determines the per diem rate?
- a) The employee's job title
 - b) The employee's travel destination
 - c) The employee's age
 - d) The employee's preferred payment method
- 11 Which of the following is NOT a commonly used expense category in Dynamics 365 Finance?
- a) Airfare
 - b) Lodging
 - c) Vehicle depreciation
 - d) Ground transportation
- 12 What is the primary purpose of the "Expense management" workspace in Dynamics 365 Finance?
- a) Managing employee payroll
 - b) Creating and submitting expense reports
 - c) Tracking customer invoices
 - d) Reviewing vendor contracts
- 13 In the context of fixed asset management, what is depreciation?
- a) An increase in the value of an asset
 - b) A decrease in the value of an asset over time
 - c) The initial cost of acquiring an asset
 - d) The value of an asset at the end of its useful life
- 14 What is the purpose of a depreciation profile in Dynamics 365 Finance?
- a) To record asset acquisitions
 - b) To calculate the depreciation of fixed assets
 - c) To manage employee salaries
 - d) To reconcile bank accounts
- 15 In Dynamics 365 Finance, what is the role of budget control?
- a) To create new budget models
 - b) To automate expense approvals
 - c) To ensure sufficient budget funds are available for planned or actual purchases
 - d) To track vendor contracts

Answers

- 1 C) *Managing bank accounts and expenses*
- 2 B) *Checks and bills of exchange*
- 3 C) *Matching bank transactions with bank statements*
- 4 C) *To deposit checks and cash into a bank account*
- 5 C) *Only if there are no pending cancellations*
- 6 A) *An agreement to pay a set amount if a customer defaults; managed in the Letter of guarantee page*
- 7 B) *Expense reports reimaged*
- 8 D) *The organization's hierarchy and financial background*
- 9 C) *Covering expenses such as meals and accommodation*
- 10 B) *The employee's travel destination*
- 11 C) *Vehicle depreciation*
- 12 B) *Creating and submitting expense reports*
- 13 B) *A decrease in the value of an asset over time*
- 14 B) *To calculate the depreciation of fixed assets*
- 15 C) *To ensure sufficient budget funds are available for planned or actual purchases*



SELF-EXAMINATION QUESTIONS FOR PRACTICE:

- 1 What are some of the key functionalities covered in the expense management module of Dynamics 365 Finance?
- 2 How does Dynamics 365 Finance handle bank account management and reconciliation?
- 3 What is the purpose of a deposit slip in the context of financial management?
- 4 Describe the major business processes associated with cash and bank management in Dynamics 365 Finance.
- 5 What is a letter of guarantee, and how does Dynamics 365 Finance assist in managing them?
- 6 How does the "Expense reports reimaged" feature improve the expense reporting process in Dynamics 365 Finance?
- 7 What factors should an organization consider during the planning phase for implementing expense management in Dynamics 365 Finance?
- 8 Explain the concept of per diems and their importance in expense management.
- 9 What are some decisions that need to be made when implementing per diems in Dynamics 365 Finance?
- 10 What is the significance of depreciation in fixed asset management, and how is it typically calculated in the system?

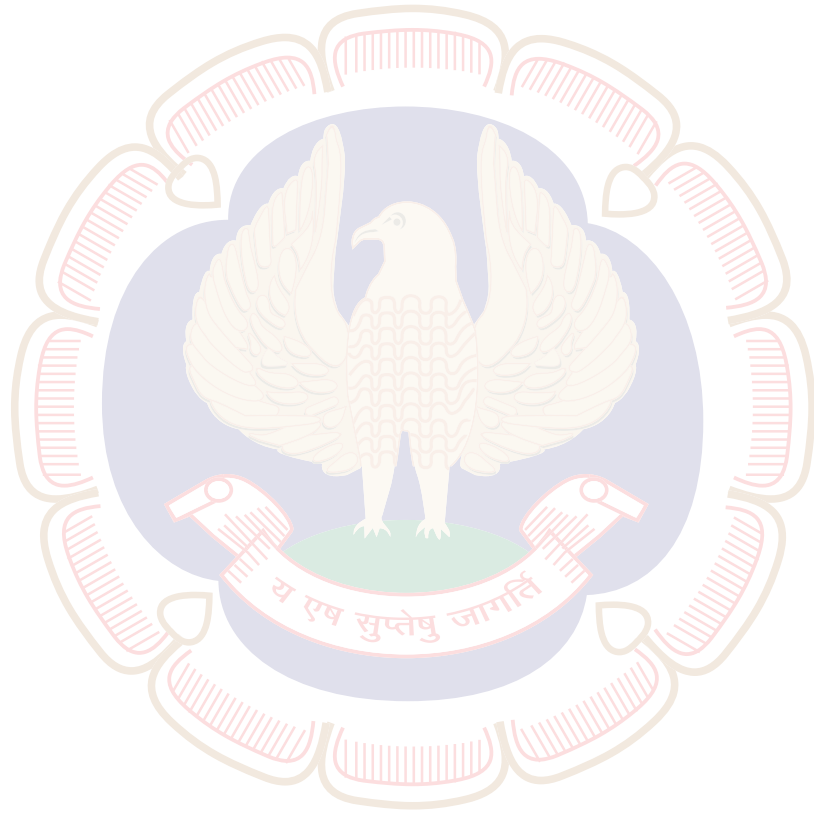
ROBOTIC PROCESS AUTOMATION

TASK STATEMENT

1. Execute basic web automation tasks.
2. Perform elementary mail automation procedures.
3. Initiate basic graphical user interface (GUI) automation.
4. Implement simple Robotic Process Automation (RPA) tasks.

KNOWLEDGE STATEMENT

1. Basic understanding of various web elements.
2. Fundamental grasp of the Selenium library for web automation.
3. Introduction to Power Automate for workflow automation.
4. Basic understanding of the SMTP library for email automation.
5. Introduction to Pandas for data manipulation and analysis.



ISBN No- 978-81-19472-79-6



Board of Studies (Academic)
The Institute of Chartered
Accountants of India

(Setup by an Act of Parliament)

ICAI Bhawan, A-29, Sector-62, Noida 201 309

Phone: 0120-3045964