CHAPTER 1

AUDITING IN ERP ENVIRONMENT

LEARNING OBJECTIVES

- To understand the requirements of SA315 and SA330 relating to IT and auditing in an ERP environment.
- To understand the types of Books of Accounts in an ERP
- To understand Controls Based audit
- To understand the difficulties in performing only Substantive audits in ERP environment
- To understand the process of Access to systems relevant for audit
- To understand the Use of work of experts in an audit

1.1 Overview

For the last 2 decades, India has been on a fast track to use Information Technology in the day to day activities. Individuals and Businesses/Corporations are increasingly dependent on IT to undertake most of their activities. Individuals using simple calculations or Corporations devising complex security features and transactions have taken the assistance of IT. While the risk of individuals using IT is limited to perhaps the individual himself, the risks of Corporations using IT are varied and have an impact on the entity, society or even the country. In such a scenario, there needs to be a check/audit on the use of IT by Corporations.

Businesses today rely on ERP systems and applications more than ever. Many of these systems generate and process data that is used in the preparation of financial statements of a company. The auditors also often rely on the data and reports that are generated from these systems. In this context, it is critical to understand the IT specific risks that could potentially impact the integrity and reliability of financial transactions and data flowing through a company's systems.

Some of the examples of ERP systems are SAP, Oracle, Peoplesoft, TALLY etc. These are available in the market and can be purchased and customised as per requirements.

In addition, the companies can develop ERP systems on their own. Companies in niche sectors like Oil and Gas etc. where the operations are complex and transactions can be different from the usual. These are categorised under Developed ERP systems.

1.2 Understand the requirements of SA315 and SA330 relating to IT and auditing in an ERP environment

SA 315 states that the objective of the auditor is to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels through,

- Understanding the entity and its control environment, including the entity's internal control framework.
- Understanding the information systems environment relevant to financial reporting and communication.
- Understanding and assessing the risks associated with the relevant environment.

The auditor will have to understand the nature of the entity and the governance structure. The governance structure will provide an indication over the Internal Control Framework. One important aspect of Control framework in an IT environment is that the entity should have separate reporting structures for the IT team and the Business team. The IT team is the owner of the application and the Business team is the owner of the data residing within the application. The roles of both the teams should be segregated and should not overlap. This communication lines are strictly drawn so as to maintain the integrity of the data within the application.

An example of the Governance framework as shown in Fig 1.2.1.

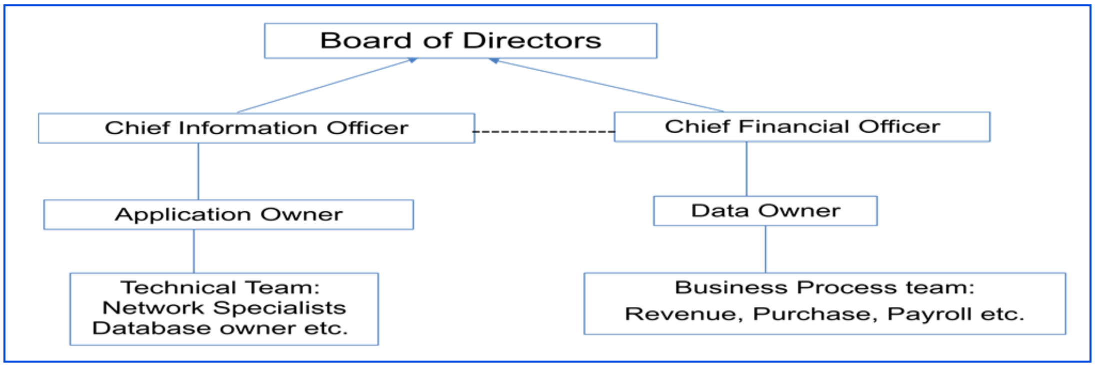


Fig. 1.2.1: Governance framework

Along with an understanding of the entity, the auditor identifies the industry to which it belongs. This will enable the auditor to get an idea of the complexity and class of transactions, account balances and disclosures to be expected in the financial statements.

The next step for the auditor is to understand the IT systems and related procedures within IT and business processes by which these transactions are initiated, recorded, processed, reported etc. These could happen within IT systems or outside.

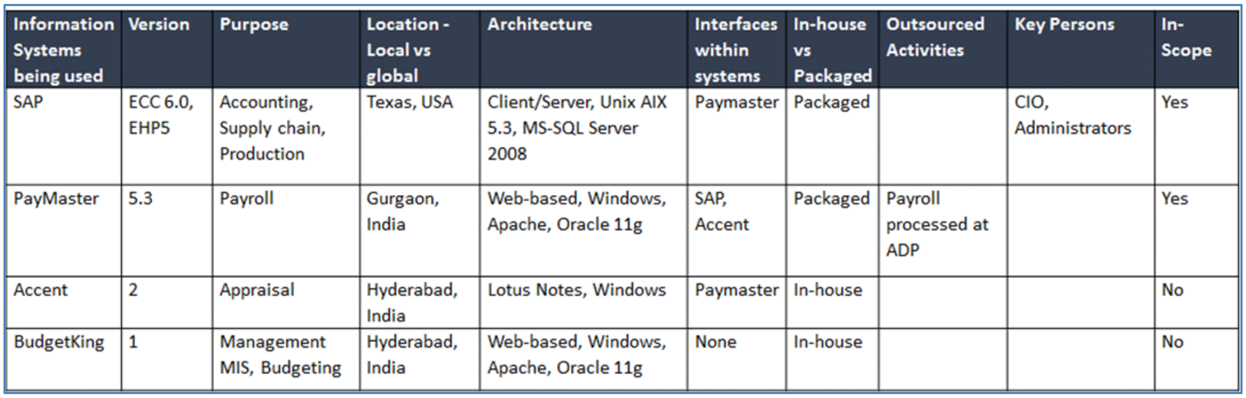
There may be instances where the events and conditions, other than routine transactions but are significant for financial reporting, may be captured in the Information Systems. We are referring to Non Standard Journal Entries. The auditor has to understand the process and controls in recording such entries.

Some examples of the Information Systems environment relevant to financial reports are given below:

1. The audit client is an entity that has many branches, depots, sales outlets across the country etc. Transactions such as invoice entries, debit/credit notes etc. may be passed at each of these locations.

2. The audit client is in the retail industry. They have many Point of Sale outlets (POS) where the sales are recorded. These POS machines should have the latest price catalogue at the time of invoicing.
3. The audit client is in the IT industry. They have many types of revenue such as milestone billing, time spent on projects etc. along with markup. This data is captured in various applications and the invoice is raised in the integrated ERP.

The information gathered during the understanding phase of the IT environment should be captured in a summary format to plan out the audit strategy.



Information Systems being used	Version	Purpose	Location - Local vs global	Architecture	Interfaces within systems	In-house vs Packaged	Outsourced Activities	Key Persons	In-Scope
SAP	ECC 6.0, EHP5	Accounting, Supply chain, Production	Texas, USA	Client/Server, Unix AIX 5.3, MS-SQL Server 2008	Paymaster	Packaged		CIO, Administrators	Yes
PayMaster	5.3	Payroll	Gurgaon, India	Web-based, Windows, Apache, Oracle 11g	SAP, Accent	Packaged	Payroll processed at ADP		Yes
Accent	2	Appraisal	Hyderabad, India	Lotus Notes, Windows	Paymaster	In-house			No
BudgetKing	1	Management MIS, Budgeting	Hyderabad, India	Web-based, Windows, Apache, Oracle 11g	None	In-house			No

Fig. 1.2.2: Audit Strategy

An example of the understanding of the Control Environment is given:

It is possible that the information flow as mentioned above may be in a partially or fully automated environment.

Automated environment refers to one with less manual process intervention and relies more on the systems driving the activities. The risks in an automated environment are many. For example, the risks may be due to the number and location of applications, interfaces between the applications, security within the applications etc. We shall learn more on the components of an Automated Environment in the sessions on General IT Controls and Automated Application Controls. However, given below are a sample of risks in an automated environment as well as an example of an IT Automated environment.

Domain	Inherent Risk of Material Misstatement	Control Description
Control Environment	Lack of segregation of incompatible IT functions/duties may lead to increased risk of fraud and unauthorized activities.	Segregation of duties has been clearly defined and documented for all critical IT functions. It is clearly communicated to all critical IT function users.
System Security	Generic users and contractor's user IDs may be used to gain unauthorized access to the network.	Generic user ID's and service accounts are identified and a "user owner" is assigned to the user ID.
System Security	Unauthorized users could access corporate data if passwords are not set according to security standards	Application, Database and Operating Systems Password controls are configured according to the Information Security Policies.

Table 1: Control Description

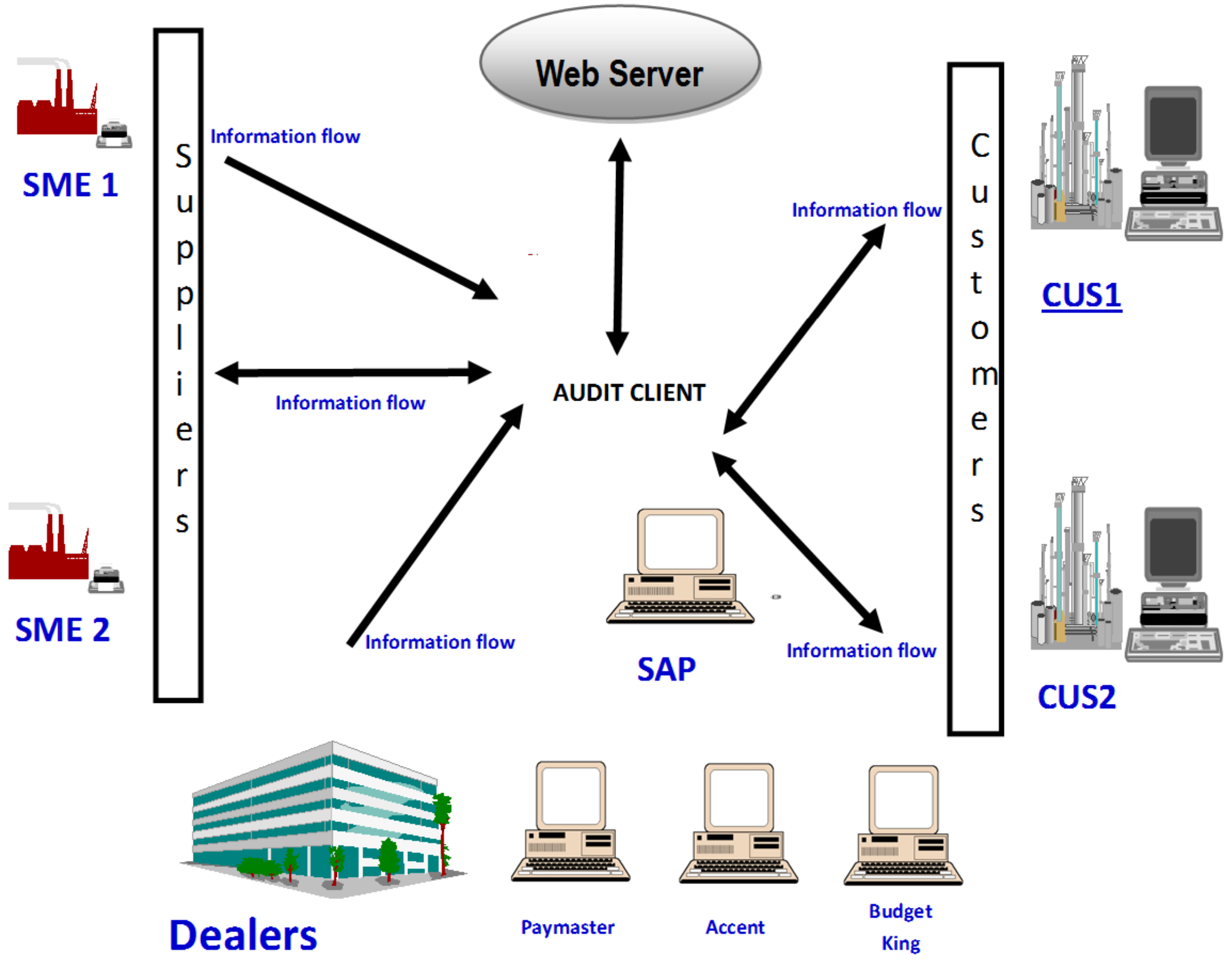


Fig. 1.2.2: IT Automated Environment

In addition to SA 315, the auditors, in response to Clause (i) of Sub-section 3 of Section 143 of the Companies Act, 2013 ("the 2013 Act" or "the Act") , have to report whether the entity has adequate internal financial controls system in place.

The auditors have to express an opinion on the effectiveness of the entity's internal financial controls over financial reporting and have also to mention the audit procedures conducted to arrive at the opinion. These procedures will be carried out along with the audit of financial statements. The requirement is applicable for listed and unlisted companies.

1.2.1 Objectives of SA 330

SA 330 deals with the auditor's responsibility to design and implement responses in the form of audit procedures in response to work done as part of SA 315. The objective of the procedures is to reduce the risk of material misstatement to an acceptable level. These audit responses will be a part of the overall audit strategy. The strategy will set the scope, timing and direction of the audit. Depending on the level of automation achieved by a Corporation, these audit procedures will revolve around a mixture of controls and substantive based approach. Such audit procedures form a part of the overall financial statement audit procedures.

Given below is the chart that explains the link between the works done as per SA 315 and SA 330 as shown in Fig 1.2.3.

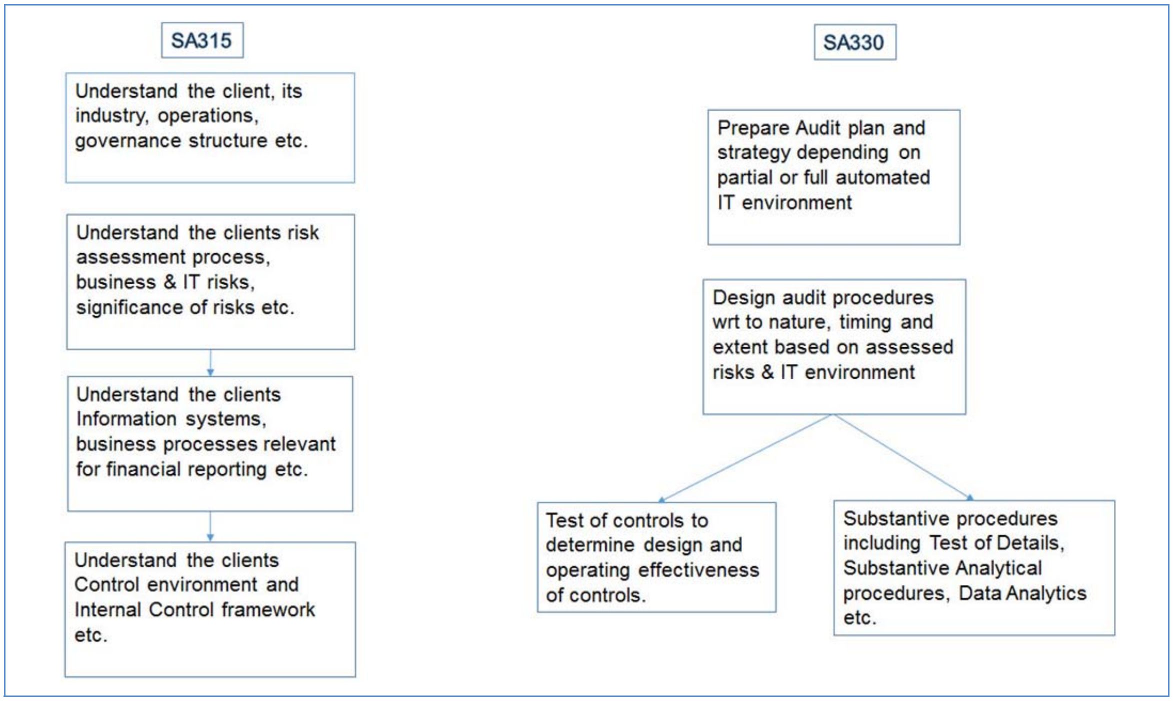

SA315
Understand the client, its industry, operations, governance structure etc.
Understand the clients risk assessment process, business & IT risks, significance of risks etc.
Understand the clients Information systems, business processes relevant for financial reporting etc.
Understand the clients Control environment and Internal Control framework etc.
SA330
Prepare Audit plan and strategy depending on partial or full automated IT environment
Design audit procedures wrt to nature, timing and extent based on assessed risks & IT environment
Test of controls to determine design and operating effectiveness of controls.
Substantive procedures including Test of Details, Substantive Analytical procedures, Data Analytics etc.

Fig. 1.2.3: The link between the works done as per SA 315 and SA 330.

Thus, the auditor as per requirements of SA 330, has to plan and execute the audit procedures to achieve the objectives of SA315 and Internal Financial Controls reporting.

1.3 Books of Accounts in an ERP

An integrated enterprise resource planning system inherently means that all the modules within the system are seamlessly connected with each other and the transactions flow through the relevant modules. Thus, there is one Primary Set of Books and all the transactions reside here.

Where the books were maintained in a manual format or in the earlier version of the systems, there were various books of accounts or ledgers. For example, there were Purchase ledgers, sales ledgers, cash book, bank book etc. Entries were passed in these books depending on the type of transactions. At the end of a period – for example on a daily basis, weekly basis or on a monthly basis, the totals of these books were posted to the General Ledger.

With the advent of ERP, such different types of books or ledgers were not used. ERP's were integrated which meant that for any type of transactions, the impact to the General Ledger was automatic and on a real time basis. The General Ledger had Control Accounts which was a summation of the respective transactions.

For example, if we take 2 purchase transactions involving 2 Vendors

Purchases Dr	- Purchase Control Account
To Vendor 1 A/c	- Creditors Control Account
Purchases Dr	- Purchase Control Account
To Vendor 2 A/c	- Creditors Control Account

In the above example, the ERP will maintain the details of transactions separately for Vendor 1 and Vendor 2 and also have a Creditors Control Account to capture the total of all Creditors balances.

The auditor, to audit the books of accounts and as per requirements of SA 330 will have to assess the risks and put in place an audit program which is a combination of

- Tests of Controls
- Substantive procedures including Substantive Analytical Procedures and Test of Details

In the below Fig 1.3.1 is given the type of audit evidence that can be obtained from the client as per SA 330 and SA 500.

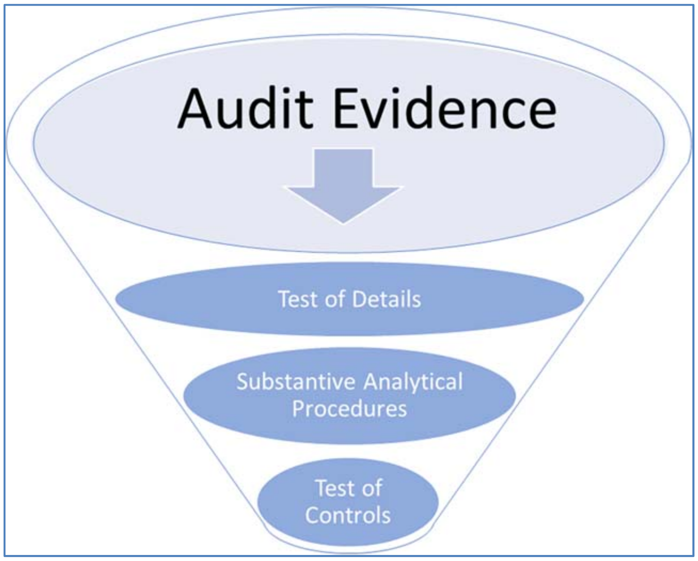


Fig. 1.3.1: Audit Evidence

While deciding on the audit procedures the auditor should take into account the risk of material misstatement at the assertion level for each class of transactions, account balance and disclosure.

1.4 Difficulties in Substantive audits in ERP

In the current automated environment, an auditor cannot devise an audit plan which is entirely made up of substantive procedures. The client may have automated complete processes in the systems to minimise or eliminate manual procedures. This increases the risk of any misstatement not being detected only by substantive procedures. Hence, the auditor will have to rely on audit procedures which include auditing within or surrounding the systems. Some other possible reasons why substantive procedures themselves may not be feasible or sufficient are:

- Increased use & complexity of Systems and Application software in Business (for example, use of old legacy systems, multiple applications)
- nature of business (Telecom, e-Commerce)
- Volume of transactions are high (Retail, Manufacturing)
- Systems distributed over different geographies(main ERP in India, Payroll application in Europe)
- Company Policy (Compliance)
- Regulatory requirements - Companies Act 2013 IFC, IT Act 2008
- Required by Indian and International Standards - ISO, PCI-DSS, SA 315, SOC, ISAE
- Outsourced processes (Part of the Purchase process outsourced to an organization outside the country)
- Increases efficiency and effectiveness of audit

1.5 Controls Based Audit

Some key aspects of SA 300 - Planning of Audit of Financial Statements, have to be taken into consideration.

- Involvement of Key Team Members – If the company/auditee is using ERP, then the audit team will have to incorporate experts/specialists in the audit team who can extract data from the ERP, navigate within the ERP, understand any rules defined by the Company within the ERP etc.
- Areas where Computer Assisted Audit Techniques - CAATS may be used as part of the audit procedures.

In determining the audit approach to include Controls Based audit, the below Fig 1.5.1 as shown the questions/criteria to be considered:

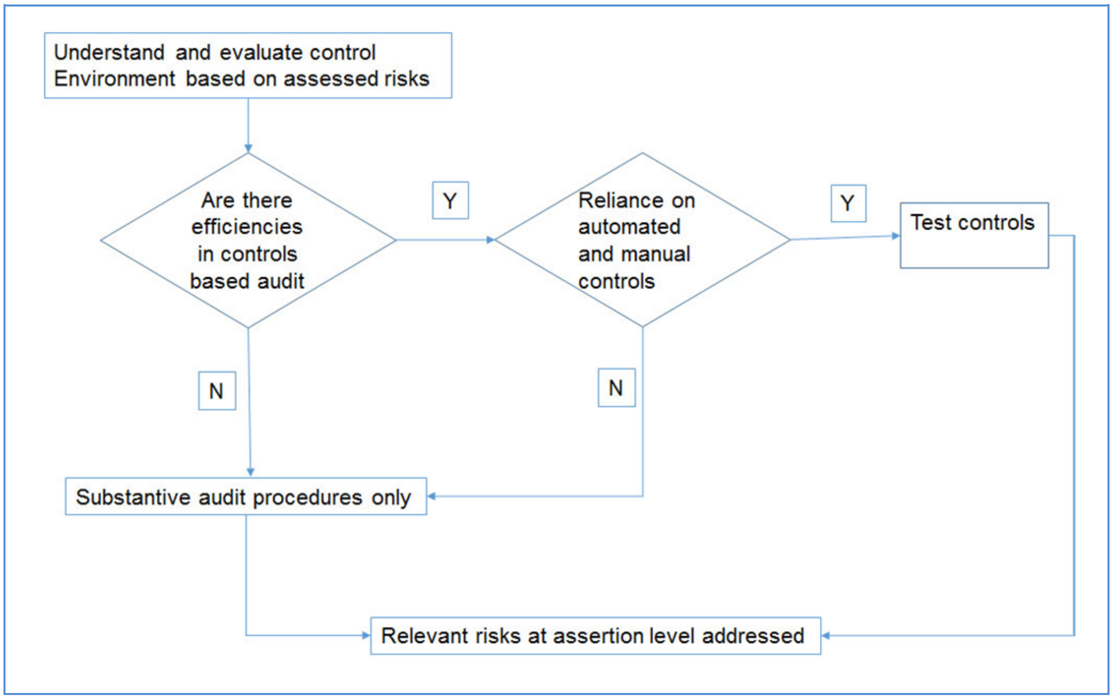

Understand and evaluate control Environment based on assessed risks
Are there efficiencies in controls based audit
Y
Reliance on automated and manual controls
Y
Test controls
N
N
Substantive audit procedures only
Relevant risks at assertion level addressed

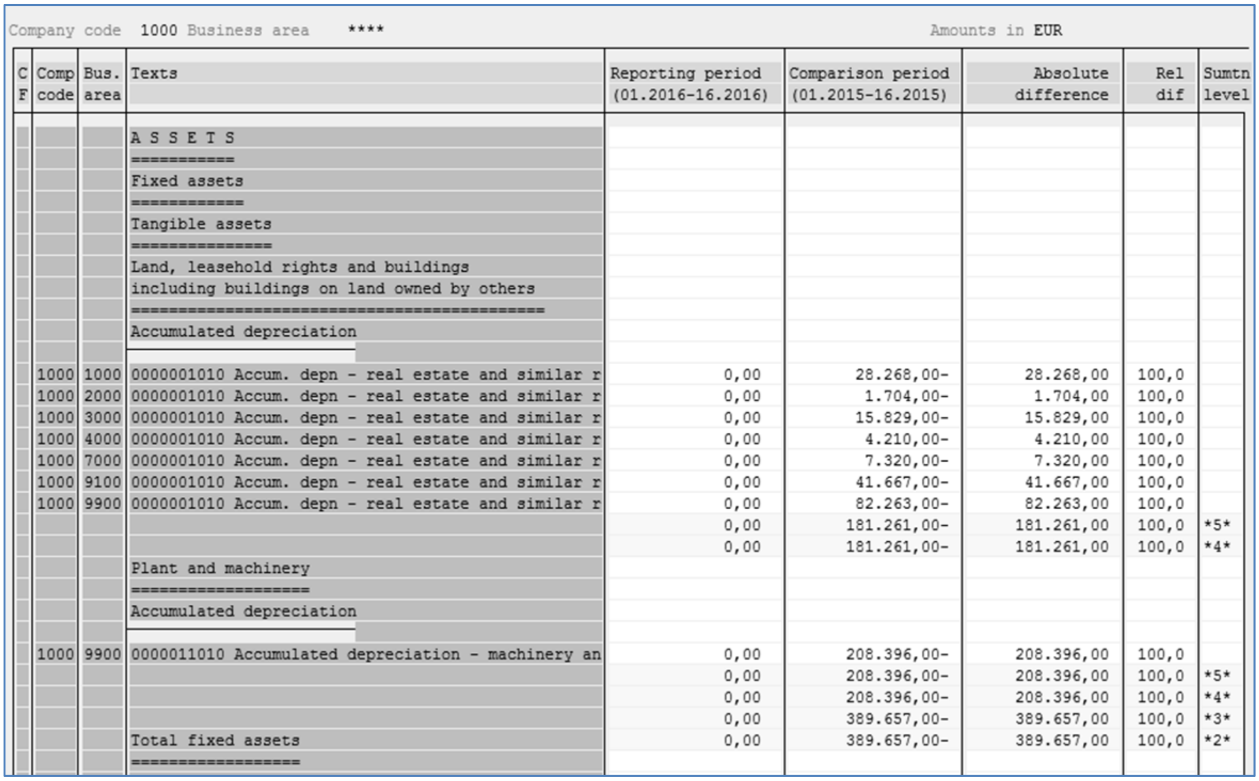
Fig. 1.5.1: Control Based Audit

The auditor after having evaluated and tested the Internal Control Framework may adopt a strategy that includes Tests of controls. The auditor may have to an appropriate mix of Controls testing along with substantive procedures. A test of controls is an **audit procedure** to test the effectiveness of a control used by a client entity to prevent or detect material misstatements. Depending on the results of this test, auditors may choose to rely upon a client's system of controls as part of their auditing activities. These controls may be manual, automated, inherent etc.

1.6 Access to systems for audit

When auditing in an ERP environment it is essential for the auditor to have access to that environment. Here are some possible reasons for requiring access to ERP

- To extract data and reports required for audit, independently. Obtaining audit data independently gives the auditor more direct audit evidence. For example, the auditor may want to get a daybook, purchase register, sales register, trial balance from an ERP system. For this purpose, the auditor should first have a user id and password to login to the ERP system of the company. The Fig 1.6.1 as shown below a sample trial balance report generated from an ERP.

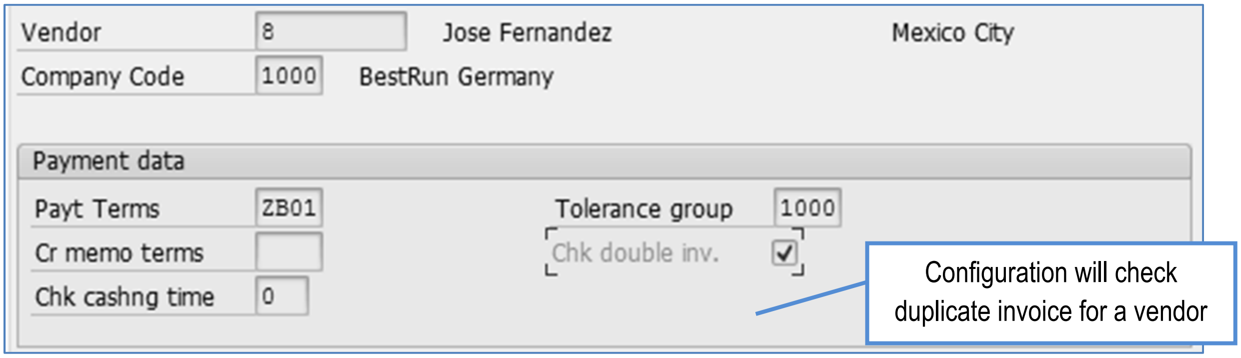


Company code 1000 Business area **** Amounts in EUR

C F	Comp code	Bus. area	Texts	Reporting period (01.2016-16.2016)	Comparison period (01.2015-16.2015)	Absolute difference	Rel dif	Sumtn level
			A S S E T S					
			===========					
			Fixed assets					
			============					
			Tangible assets					
			===============					
			Land, leasehold rights and buildings					
			including buildings on land owned by others					
			==					
			Accumulated depreciation					
	1000	1000	0000001010 Accum. depn - real estate and similar r	0,00	28.268,00-	28.268,00	100,0	
	1000	2000	0000001010 Accum. depn - real estate and similar r	0,00	1.704,00-	1.704,00	100,0	
	1000	3000	0000001010 Accum. depn - real estate and similar r	0,00	15.829,00-	15.829,00	100,0	
	1000	4000	0000001010 Accum. depn - real estate and similar r	0,00	4.210,00-	4.210,00	100,0	
	1000	7000	0000001010 Accum. depn - real estate and similar r	0,00	7.320,00-	7.320,00	100,0	
	1000	9100	0000001010 Accum. depn - real estate and similar r	0,00	41.667,00-	41.667,00	100,0	
	1000	9900	0000001010 Accum. depn - real estate and similar r	0,00	82.263,00-	82.263,00	100,0	
				0,00	181.261,00-	181.261,00	100,0	*5*
				0,00	181.261,00-	181.261,00	100,0	*4*
			Plant and machinery					
			====================					
			Accumulated depreciation					
	1000	9900	0000011010 Accumulated depreciation - machinery an	0,00	208.396,00-	208.396,00	100,0	
				0,00	208.396,00-	208.396,00	100,0	*5*
				0,00	208.396,00-	208.396,00	100,0	*4*
				0,00	389.657,00-	389.657,00	100,0	*3*
			Total fixed assets	0,00	389.657,00-	389.657,00	100,0	*2*
			==================					

Fig. 1.6.1: A sample trial balance report generated from an ERP.

- To test automated application controls through the system by inspection of configurations. For example, consider a solution of a situation where duplicate vendor invoices are automatically identified and blocked in the ERP system. To test this automated control, the auditor needs to review the relevant configurations or settings in the ERP . The auditor will require access to ERP for carrying out this test of control. Refer below screenshot of configuration for duplicate invoice check in ERP application as shown in Fig 1.6.2.



Vendor	8	Jose Fernandez	Mexico City
Company Code	1000	BestRun Germany	

Payment data

Payt Terms	ZB01	Tolerance group	1000
Cr memo terms		Chk double inv.	☑
Chk cashng time	0		

Configuration will check duplicate invoice for a vendor

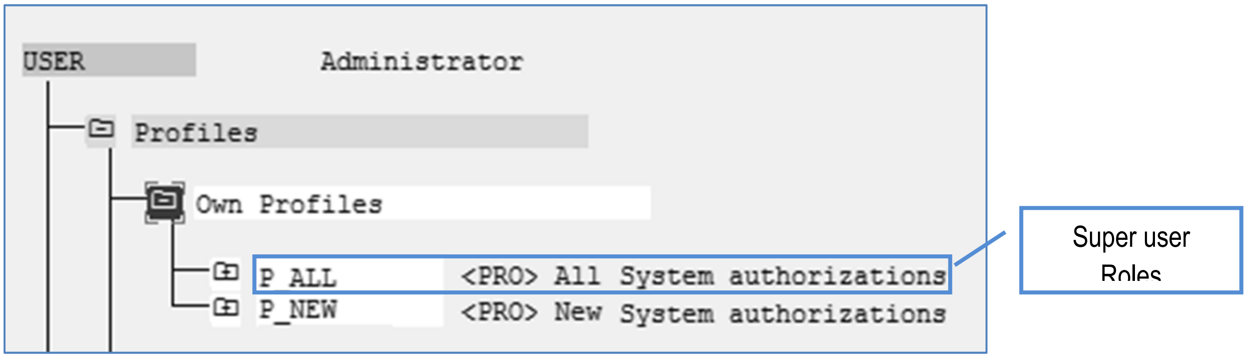
Fig. 1.6.2: Configuration for duplicate Invoice Check an ERP.

When auditors have access to systems, it makes the audit process more efficient and effective and also reduces the amount of time the company staff have to devote for audit. However, there are certain points to remember when requesting for access to systems. They are,

- Auditors should always request access to the production or live environment. Production environment is where business transactions are posted, financial statements including trial balance, balance sheet and profit & loss statements are generated. Access to non-production environments alone viz., quality, test systems will not suffice unless additional audit evidence is obtained to corroborate that data obtained from non-production systems is consistent with the production system data. We will learn more about the various system environments in the chapters on General IT Controls.

- The type of access that auditors request should be Display-Only or Read-Only i.e., access without the ability to create, alter or delete data in the ERP environment. This is essential because auditors should not make changes to business data, even inadvertently.

- Super user, privileged or administrative access is not always necessary for auditors and should not be requested. Even when provided with super user, privileged or administrative access to systems, it is better to decline acceptance of such access. For example, in SAP ERP the users who are assigned the role SAP_ALL or SAP_NEW have super user access which means these users can perform any transaction or activity in the ERP. This level of super user access is generally not necessary for an auditor.



```
USER            Administrator
  Profiles
    Own Profiles
      P_ALL       <PRO> All System authorizations
      P_NEW       <PRO> New System authorizations
```

Super user Roles

Fig. 1.6.3: Super user Roles

- Auditor should request for temporary access for the duration of audit to minimise any possible misuse of the same access at a later date.

- Prior to obtaining access to company systems, the auditor should receive sufficient training or orientation in navigating through the systems and applications. Experimenting on company systems should be avoided. In case the auditor does not have sufficient knowledge of an ERP, they should take help from experienced and authorised users of the ERP.

- To obtain data from core technology components of an ERP environment viz., operating systems, databases, networks, the auditor should take help from the respective administrators of those systems.
- Before obtaining access to systems, the auditor should also gain an understanding of the company IT policies including password policy, user access policy and acceptable usage policy and so on. For example, complexity, duration and length of passwords etc. This is essential so that the auditor does not inadvertently violate the company policies or compromise IT security.

1.7 Involvement of experts

When auditing in an ERP environment, it is likely that the auditor will come across certain aspects of and ERP environment that require more in-depth understanding and knowledge of the technical subjects. Examples of what an auditor may have to looking at and review could include,

- Complex ERPs like SAP
- Legacy systems including mainframes and AS/400 systems
- Latest technology like cloud computing
- In-house developed systems and applications
- Customised and specialised systems
- Database like Oracle or SQL Server
- Operating systems like Unix and variants

To determine the scope, understand the ERP environment, assess risks and carry out audit tests will require special training, expertise and skills for an auditor (of financial statements). In certain cases where the auditor may not possess such knowledge and skills an expert should be involved. Just like how auditors sometimes involve experts from the fields of Taxation, Transfer Pricing, Valuators, Actuaries, even IT specialists can be involved as experts in an audit of financial statements. The standard SA 610 - Using the Work of an Auditor's Expert provides the necessary guidance on involving experts.

1.8 Exercise

1. _________ states that the objective of the auditor is to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels.
2. Understanding the information systems environment relevant to financial reporting and communication is a part of:

   (a) SA300

   (b) SA315

   (c) SA330

   (d) SA500
3. The __________ team is the owner of the application.

4. The __________ team is the owner of the data within the application.
5. In response to Clause ___ of Sub-section __ of Section 143 of the Companies Act, 2013, the auditor has to report whether the entity has adequate internal financial controls system in place.
6. ______ deals with the auditor's responsibility to design and design and implement responses in the form of audit procedures in response to work done as part of SA 315.
7. Involvement of key team members and usage of CAATS is a part of SA _______, Planning of Audit of Financial Statements.
8. Involvement of Experts in audit is covered under SA ______.
9. Complexity, duration and length of passwords are a part of :
   (a) User access policy
   (b) Password policy
   (c) Acceptable usage policy
   (d) None of the above.
10. Typically, the auditors should request for ___________ access or ___________ access to the client's ERP system.

1.9 Glossary

ERP – Enterprise Resource Planning

POS – Point of Sale

GITC – General Information Technology Controls

CAATS – Computer Assisted Audit Techniques

ISO – International Organisation for Standardisation

PCI-DSS – Payment Card Industry – Data Security Standard

ISAE – International Standard for Assurance Engagements

SOC – Service Organisation Controls

1.10 References and other reading material

1. Standards on Auditing published by the Institute of Chartered Accountants of India (ICAI), www.icai.org > Resources
2. Guidance Note on Audit of Internal Financial Controls Over Financial Reporting issued by Auditing and Assurance Standards Board. - (14-09-2015), www.icai.org
3. Companies Act 2013, www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf

1.11 Answer to Exercise

1. SA 315
2. Answer is b – SA 315.
   - SA 315 mentions that it is key to understand the information systems environment relevant to financial reporting and communication.
3. IT Team
4. Business team
5. Clause (i) of Sub-section 3 of Section 143 of the Companies Act, 2013
6. SA330
7. SA 300
8. SA 610
9. Answer is b – Password policy
10. Display only or Read only

CHAPTER

2

GENERAL INFORMATION TECHNOLOGY CONTROLS

LEARNING OBJECTIVES

- To understand about General IT Controls
- To understand the categories and types of General IT Controls
- To understand the impact of General IT Controls on Audit of financial statements
- To know which systems to scope for review of General IT Controls
- To learn about the sample size requirements for General IT Controls
- To understand the procedures for review of various categories or domains of General IT Controls including IT Governance, Program Changes, Access Security, Data center and network Operations, Application system acquisition, development and maintenance
- To understand how to evaluate impact of deficiencies in General IT Controls on overall audit
- To know when to test General IT Controls

2.1 What are General IT Controls

"General IT controls are policies and procedures that relate to many applications and support the effective functioning of application controls. They apply to mainframe, miniframe, and end-user environments. General IT-controls that maintain the **integrity** of information and **security of data** commonly include controls over the following:" (SA 315)

These are IT controls generally implemented to mitigate the IT specific risks and applied commonly across multiple IT systems, applications and business processes. Hence, General IT controls are known as "pervasive" controls or "indirect" controls.

2.2 Categories of GITCS

There are basically four categories of General IT Controls which are as follows:

- Data center and network operations
- Program change
- Access security
- Application system acquisition, development, and maintenance (Business Applications)

In addition to the above there are aspects of that relate to the governance and oversight of IT systems at the entity level known as IT Governance. The auditor is required to obtain an understanding of IT Governance as part of the review of Entity Level Controls.

2.3 Types of Controls

The different types of controls are as follows:

Automated Controls

Automated controls are embedded into IT applications viz., ERPs and help in ensuring the completeness, accuracy and integrity of data in those systems. Examples of automated controls include edit checks and validation of input data, sequence number checks, user limit checks, reasonableness checks, mandatory data fields, user access controls and password controls.

Manual Controls

Manual controls are activities in a business process that are performed by individuals or employees manually i.e., without the need to rely on a IT system or data generated by a system. For example, manual controls include approval of a manual journal voucher, reviewing reconciliations, authorisation for payments, approving credit limits and segregation of duties, user acceptance testing of program changes.

IT-Dependent Controls

IT dependent controls are basically manual controls that make use of some form of data or information or report produced from IT systems and applications. In this case, even though the control is performed manually, the design and effectiveness of such controls depends on the reliability of source data.

2.4 How do GITCS Impact Audit

When IT systems are used in a company for processing of business transactions and activities there will be risks which are specific to the use of IT systems that need to be considered. Examples of IT risks are given below:

- Inaccurate processing of data, processing inaccurate data, or both
- Unauthorized access to data
- Direct data changes (backend changes)
- Excessive access / Privileged access (super users)
- Lack of adequate segregation of duties
- Unauthorized changes to systems or programs
- Failure to make necessary changes to systems or programs
- Loss of data

The auditor should identify, evaluate and assess the IT risks to determine impact on audit. General IT Controls or GITCs are internal controls that are implemented by a company to mitigate IT risks. Effective implementation and operation of General IT Controls are essential for relying on the following:

- Information Produced by Entity (IPE) i.e., data, information or reports that are generated from systems
- Automated controls, calculations, accounting procedures that are built into the applications
- IT dependent controls

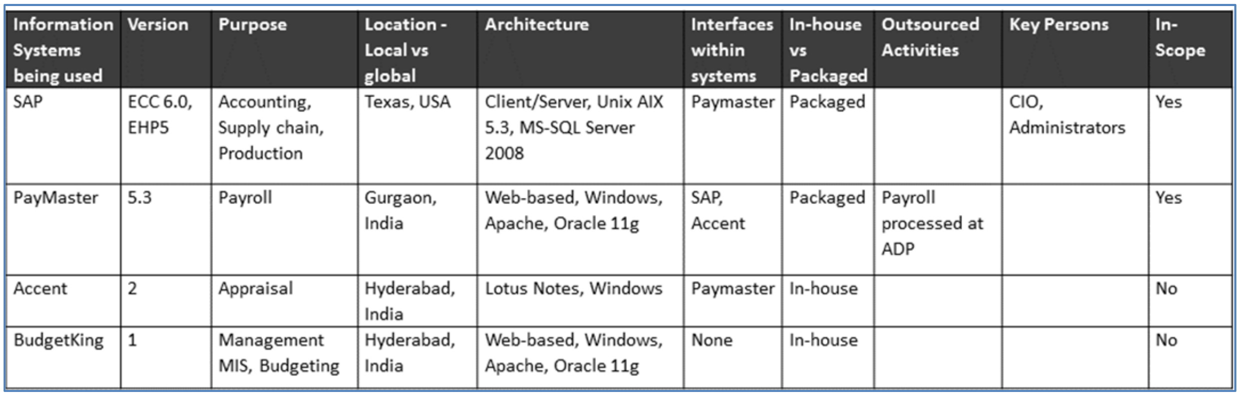
Due to the inherent dependency on IT, the effectiveness and reliability of Automated controls and IT dependent controls require the General IT Controls to be effective.

2.5 Which Systems to Scope for Review of GITCS

In an audit of financial statements, the auditor is required to understand the entity and its business, including IT as per SA 315. As mentioned in the introduction section, obtaining an understanding of a company and its automated environment involves understanding how IT department is organised, IT activities, the IT dependencies, relevant risks and controls. Depending on the nature, size and complexity of operations, a company could be using one or more IT systems and applications.

While the auditor is required to obtain an understanding, document the IT environment at a company, including all IT systems, the auditor is required to consider only those General IT Controls that mitigate risks relevant to financial statements.

Which IT systems and General IT Controls to include in-scope for an audit depends on the auditors' judgement and assessment of risk of material misstatements to financial statements and the planned audit response to these risks.



Information Systems being used	Version	Purpose	Location - Local vs global	Architecture	Interfaces within systems	In-house vs Packaged	Outsourced Activities	Key Persons	In-Scope
SAP	ECC 6.0, EHP5	Accounting, Supply chain, Production	Texas, USA	Client/Server, Unix AIX 5.3, MS-SQL Server 2008	Paymaster	Packaged		CIO, Administrators	Yes
PayMaster	5.3	Payroll	Gurgaon, India	Web-based, Windows, Apache, Oracle 11g	SAP, Accent	Packaged	Payroll processed at ADP		Yes
Accent	2	Appraisal	Hyderabad, India	Lotus Notes, Windows	Paymaster	In-house			No
BudgetKing	1	Management MIS, Budgeting	Hyderabad, India	Web-based, Windows, Apache, Oracle 11g	None	In-house			No

Fig 2.5.1: IT environment

In this example, the auditor has obtained an understanding if IT environment which has four different IT applications being used at a company. However, the auditor has considered two applications i.e., SAP and Paymaster as "In-Scope" for audit since these two applications are used in the processing of financial transactions which has a direct impact on the accounting and preparation of financial statements.

However, two other applications "Accent" and "BudgetKing" are not considered in scope for audit because these systems, even though are important for the company, do not impact the financial data and accounting of the company.

2.6 Sample Size

The methodology and approach for testing General IT Controls in an audit of financial statements is the same as approach for testing other internal controls including manual controls, automated controls or IT-dependent controls. Accordingly, the sample size requirements when testing General IT Controls are also the same. The considerations for determining sample size include the following:

- Size of population to test
- Type of control - Manual/Automated/IT-Dependent
- Frequency of control - Daily/Weekly/Monthly/Quarterly
- Nature of test - Inquiry/Observation/Inspection/Reperformance
- Timing of test - Interim/Year-end/Full Period
- History of errors and exceptions
- Tolerance for exceptions
- Effectiveness of Entity Level Controls
- Risk assessment - High/Medium/Low

The auditor should apply professional judgement in determining the sample size for testing controls and is required to explicitly document the following as per SA 230,

- factors considered and justification for sample size
- how the auditor ensured completeness of population

2.7 Procedures for Review of IT Governance

IT Governance is a part of the larger corporate governance of a company that involves establishment of the IT framework in a company which includes

- Defining IT objectives
- Alignment of IT objectives with business objectives
- Setup IT organisation structure
- Define Roles & Responsibilities of IT personnel
- Create IT policies and processes
- Monitor quality and effectiveness of IT

In an audit of financial statements, the auditor is required to understand and evaluate the internal controls components other than control activities i.e., Control Environment, Risk Assessment, Information & Communication and Monitoring as a part of reviewing Entity Level Controls. The Information & Communication component requires the auditor to obtain an understanding of

- how business processes operate,
- the relevant information systems used in the processing of business transactions and activities,
- the risks and controls pertaining to the information systems and underlying infrastructure
- reliability of information generated from systems

While Information & Communication is more relevant to the use of information systems in a company, in large and complex ERP environments it is likely that the other components of internal controls viz., Control environment, Risk assessment and Monitoring will also be relevant.

The following is a sample procedure of how the auditor performs an understanding and evaluation of the IT Governance in a company.

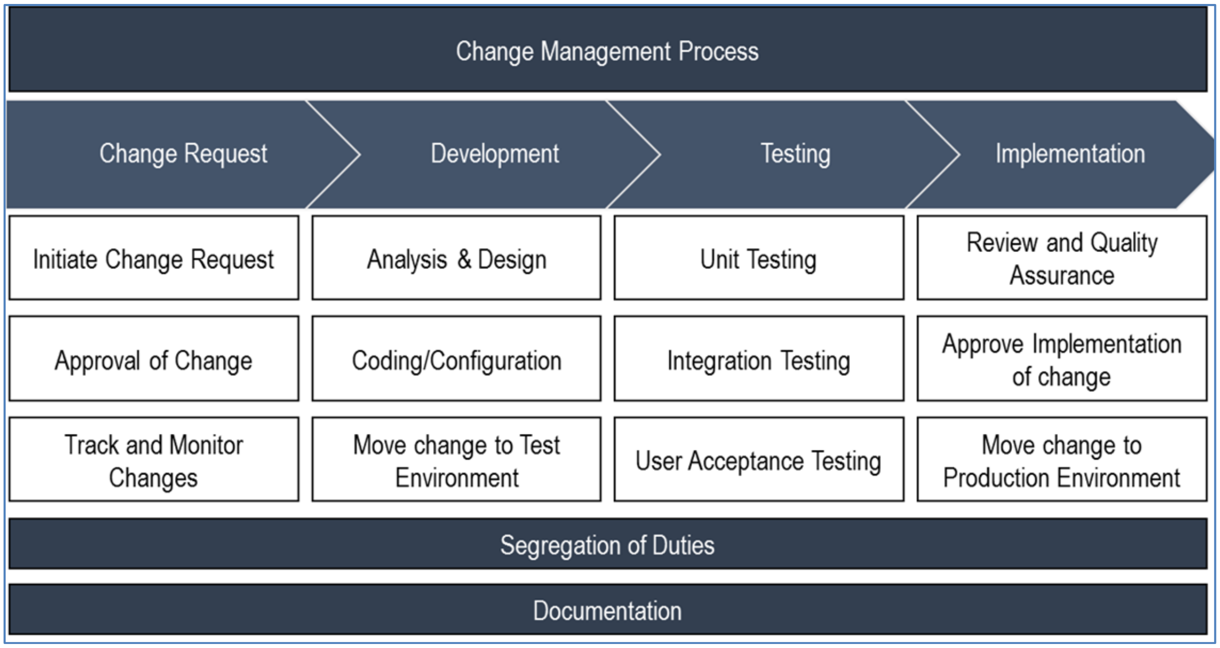
Ref No.	IT Governance Review Checklist
1	How is the IT department organised
2	Who has ownership and provides leadership for IT function
3	The manner in which IT function reports to those charged with governance i.e., Board of Directors/Audit Committee
4	Have formal IT policies and procedures been defined
5	Are roles and responsibilities defined and assigned to IT personnel
6	Is there segregation of duties within key IT functions
7	Do human resource policies and process ensure that right people are hired for key IT functions
8	Is security training and awareness provided to employees
9	How does IT communicate and collaborate with other business functions
10	What is the process for identifying and addressing IT risks
11	How does the company ensure the reliability, effectiveness of IT systems
12	Is compliance with and adherence to IT policies and procedures monitored and measured

Table 1: IT Governance

2.8 Procedures for Review of Program Changes

The Program changes domain of General IT Controls involves the understanding and evaluating the process, risks and controls that are relevant to making changes to the IT systems and applications.

The objective of program changes is “To ensure that modified systems continue to meet financial reporting objectives”. The change management process and activities in the process can be understood from the illustration as shown in Fig 2.8.1:



Change Management Process

Change Request	Development	Testing	Implementation
Initiate Change Request	Analysis & Design	Unit Testing	Review and Quality Assurance
Approval of Change	Coding/Configuration	Integration Testing	Approve Implementation of change
Track and Monitor Changes	Move change to Test Environment	User Acceptance Testing	Move change to Production Environment

Segregation of Duties

Documentation

Fig 2.8.1: The change management process

The process for program changes is similar to the process that is followed for acquisition, development and implementation of new systems. The program change process begins after a new system or ERP is implemented and involves the ongoing maintenance of ERP system. In other words, program changes process begins from the point where program development ends i.e., after go-live stage.

- **Change Requests**: A user initiates a request for change based on a business requirement. For example, a new report may be required because of a regulatory requirement or for internal reporting. The change request is reviewed and approved by a supervisor or head of department. All changes are recorded and tracked to ensure timely completion.

  There are different types of changes including the following:

  - Normal changes – these are changes required in the existing functionality of the ERP due a business need.
  - Bug fixes – a bug is an error in software which affects business transactions or reports in an ERP. Changes are required to be made to the program or configuration of the ERP to rectify or fix the bug. Identification of bugs normally happens when a user reports a problem to the IT Helpdesk. In such cases it is likely that a request made to helpdesk is converted to a program change request by the IT department and approval is provided by a IT Manager or ERP consultant instead of the supervisor of business user.
  - Enhancements – when new improvements or functionality is added to an existing ERP. For example, a workflow process is introduced for processing purchase orders to facilitate system based approvals.

  - Minor changes – changes that take less time and effort are classified as minor changes. For example, any program change that requires less than 40 hrs of effort may be considered as minor change.
  - Major changes – these are changes that require more time and effort to develop and implement. For example, changes that take more than 100 hrs of effort may be considered as major change.

    Sometimes where major enhancements and major changes take place in an ERP, such changes may fall under the GITC domain of Program development instead of program changes.
  - Patches and updates – these are changes provided by the vendor of ERP to address known bugs, security, or provide improvements to functionality to existing ERP.

    Patches and updates are typically initiated and processed by the IT department. Depending on the nature of the patch or update, the business user involvement could vary.
  - Data changes – these are direct changes to data carried out in the backend database using SQL statements or tools.

    Direct data changes are high risk because they bypass the application controls and directly impact integrity of financial data.
  - Emergency changes – these are changes that are required to be carried out urgently to prevent disruption to business transactions. For example, an emergency change is required to fix a bug that impacts critical business transaction viz., invoice / despatches or patches released by ERP vendor to address a security vulnerability found in the ERP.

    Due to the nature of emergency changes, it is likely that the change management process may be bypassed for implementing the change. However, the necessary approvals and documentation should be obtained subsequently within a reasonable time frame.
  - Changes in IT Infrastructure – These are changes made to the IT infrastructure components that support the ERP. For example, upgrades in operating system or database, changes to network configuration, installation of new hardware, etc.

    Infrastructure changes are technical in nature and do not affect the business functionality. These changes are initiated and processed by the IT department.

- **Development**: Approved change requests are provided to the IT department where the systems analysts perform analysis & design and prepare the functional / technical requirement specification for the change. The programmers develop the change by writing the program code or modify the configuration in the development environment. Once development is completed, the change is moved to test environment for testing.
- **Testing**: Program changes are tested to verify that a change works as intended. Testing is done at different levels. Unit testing is done by developer to test the working of specific change made. The functional consultant tests the change by preparing test cases and test scripts to simulate different scenarios and verify if the change meets the functional specifications under all scenarios including integration with other modules and interfaces to other systems, if any. Business user, who initially

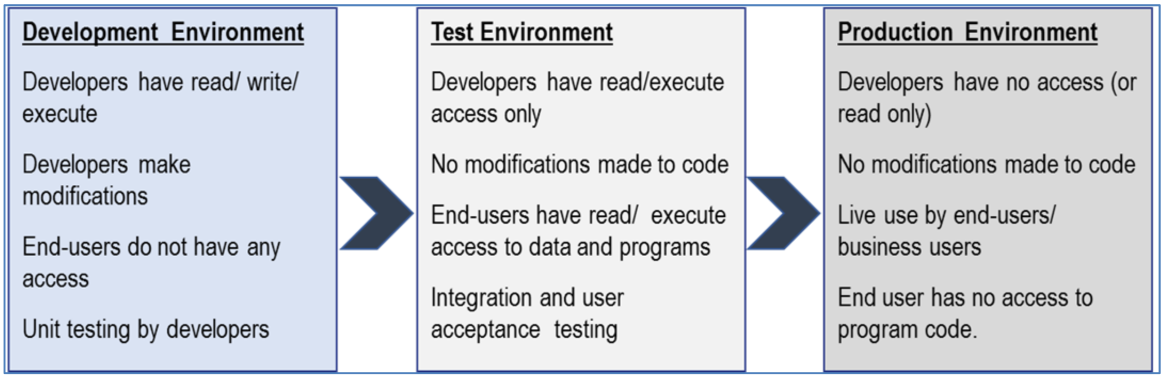
requested the change, performs the user acceptance testing to verify that a program change meets business requirement for which change request made.

The extent of testing a program change could vary depending on the nature of the change itself. For example, a change in existing report format and layout may not require extensive testing, whereas a new report that is developed may require more testing. Bug fixes and other IT specific changes may require unit testing and integration testing, but not user acceptance testing.

- **Implementation**: Prior to implementing changes in production environment, a quality assurance team reviews the changes and documentation prepared for adherence to company's change management process. After clearance is obtained from quality assurance, the IT head or equivalent approves the implementation of change in production environment based on which an administrator moves the change from test to production environment.

  In case of major changes or enhancements that impacts a larger user group, training and awareness of change should be provided to users.

- **Segregation of duties**: The change management process requires several tasks to be carried out by different people in different environments viz., development, test and production. These tasks and environments should be adequately segregated to prevent unauthorised changes from being made. The illustration as shown in Fig 2.8.2 below is an example of how this segregation can be implemented.



Development Environment

Developers have read/ write/ execute

Developers make modifications

End-users do not have any access

Unit testing by developers

Test Environment

Developers have read/execute access only

No modifications made to code

End-users have read/ execute access to data and programs

Integration and user acceptance testing

Production Environment

Developers have no access (or read only)

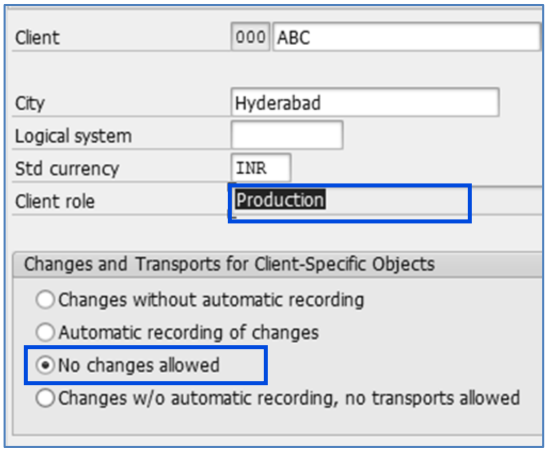
No modifications made to code

Live use by end-users/ business users

End user has no access to program code.

Fig 2.8.2: Segregation of duties

Example of configuration to prevent direct changes in ERP production environment:



Client	000 ABC
City	Hyderabad
Logical system	
Std currency	INR
Client role	Production

Changes and Transports for Client-Specific Objects

- ○ Changes without automatic recording
- ○ Automatic recording of changes
- ● No changes allowed
- ○ Changes w/o automatic recording, no transports allowed

Fig 2.8.3: To prevent direct changes in ERP

Example showing three separate environments for development (SBD), testing (SBQ) and production (SBP) in Fig 2.8.3

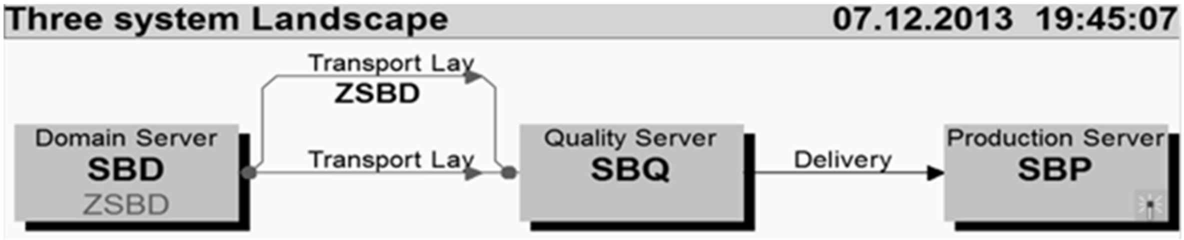


Fig 2.8.3: Three separate environment for development, testing and production

Documentation: Sufficient and appropriate documentation should be prepared and maintained to support all program changes. The documentation should include the following,

- change request forms
- approvals and sign-offs
- source code
- test cases and test scripts with results obtained
- user acceptance testing outputs and results
- record of training provided to users
- updates to user manuals and technical manuals to reflect the changes

The below illustration is an example of change request form

ABC Private Limited

Change Request in ERP

Project Name		**CR No**	
Project Id		**CR Date**	
Requestor		Request No.	
Designation		Request Date	
Contact Number			
E-Mail Id			

Sl. No.	Application	Module/Functionality/ Screen	Change Request Details	Proposed Changes	Status
1					

Requested by (Sign, Name & Date)	**HOD / In-Charge** (Sign, Name & Date)	**UAT Sign-off** (Sign, Name & Date)
Developed by (Sign, Name & Date)	**Change Implemented by** (Sign, Name & Date)	**IT In-Charge / IT Head** (Sign, Name & Date)

The table below has examples of risk and controls that an auditor may consider when reviewing program changes

Ref No.	Activity	Risk	Control description
1	Change Request	Unauthorised changes are processed	The change request is approved by the department In-charge or Head of department (HOD). Changes to IT infrastructure components are approved by IT Head.
2	Testing	Untested changes could compromise the integrity of financial data	Unit testing is performed by developer, user acceptance testing is done by end user prior to implementing in production environment.
3	Segregation of duties	Changes are made directly in production environment and may result in loss of data	Three separate environments exist for development, quality (test) and production. Separate teams are involved in development and migration of changes to production.

Ref No.	Activity	Risk	Control description
		and program integrity.	Development of changes is done by consultants and movement of changes to production is performed by System Administration only after approval.
4	Implementation	Changes are implemented by unauthorised persons.	Access to migrate changes to production is restricted to System Administrators only.
5	Documentation	Changes are applied bypassing the change management process.	A monthly review of all changes to application programs is performed by internal audit/quality assurance team. Exceptions and deviations are reported to senior management and those charged with governance.

Table 2: Risk & Control description

2.9 Procedures for Review of Access Security

Access security is one of the categories or domain of General IT Controls that involves the understanding and evaluating the process, risks and controls that are relevant to user access and security configurations in the IT environment.

The objective of access security domain is “To ensure that access to programs and data is authenticated and authorized to meet financial reporting objectives”. The access security is implemented at several layers of the IT environment as shown in Fig 2.9.1.

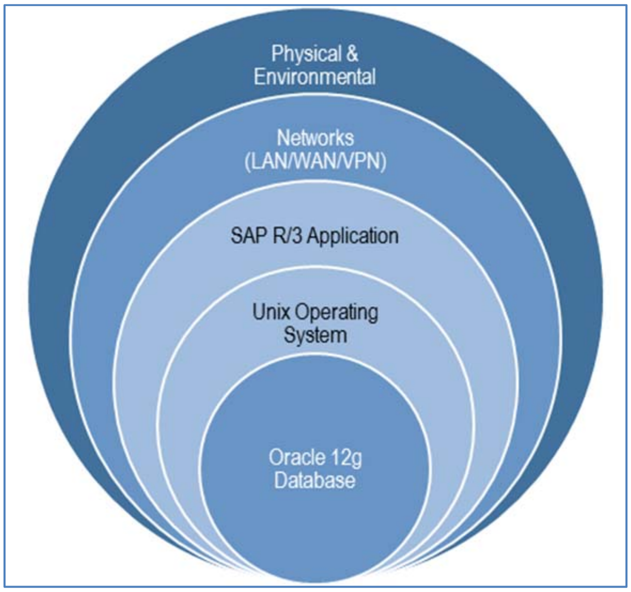


Fig 2.9.1: Access security

The various activities in this domain include the following:

- **User management**: involves granting, modification and revocation of user access and periodic review of user access to ensure that access granted is consistent with user job responsibilities and excessive access is not granted. For example, when a new employee joins a company in the stores department, a new user id is created and granted access to company network and ERP to process goods movements.

  In case existing employee in accounts payables section is promoted as finance manager and transferred to from factory office to head office, his/her access in ERP should be modified by removing access to process accounts payables transactions at plant/factory and providing access to approve payments at head office level.

  When an employee resigns and leaves a company, access of the employee should be revoked/removed from network, ERP application and office premises without delay.

  User management apply to all layers of access security i.e., application, database, operating system, network and physical layers because users are created, modified and revoked at all layers.

- **Sensitive Access and Segregation of Duties (SA/SoD)**: involves granting user the ability to perform critical business activities in an ERP. Segregation of duties refers to the identification of conflicting business activities and preventing users from being granted to access these conflicting activities. The chapter “Segregation of Duties and Sensitive Access” gives a detailed explanation with examples about SA/SoD at ERP application layer.

  Apart from the application layer, SA/SoD is relevant at other layers of security. Examples of how sensitive access and segregation of duties is implemented (for other than application layer) in an IT environment are as follows,

  - In modern client/server and web-based applications, business users are generally not created at the database and operating system layers. However, some companies could be using legacy systems in which user access may be created at database and/or operating systems.
  - Only administrators, or IT operations personnel should be granted access to database, operating system and network layers for day-to-day management of IT operations, not business users.
  - Developers and programmer access should be restricted to development environment and testing environments. Developers should not have access to production environment.

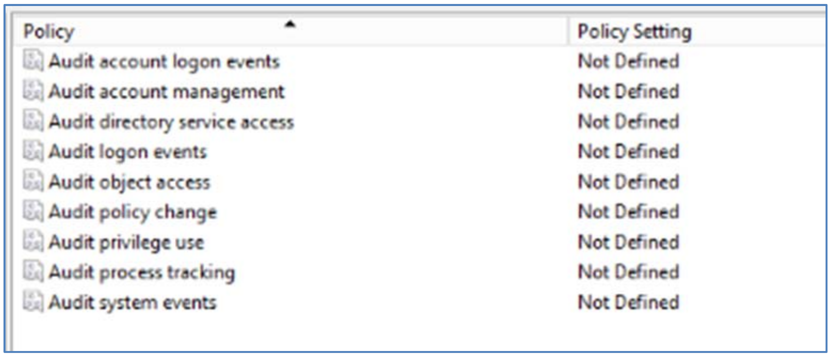
- **Privileged user access**: commonly known as super users or admin users, a privileged user is someone with full or unlimited access to IT systems or applications. Privileged users may exist at all layers of access security. Typically, these users are system administrators, database administrators or network administrators. Because of the excessive level of access, it may not be possible to enforce security controls viz., SA/SOD for privileged users and hence privileged user access is considered high risk. Hence, activities of these users should be logged and reviewed periodically.

- **Audit logging and monitoring**: an audit log or audit trail is a historical record of events and activities that take place in an IT environment. Audit logs are relevant to all layers of access security. In most IT systems and applications, enabling audit log is an optional feature and must be explicitly enabled and configured appropriately. Audit logs can quickly grow in size and occupy high volume of data and storage space and likely to impact performance of a system. However, some systems including, Windows

Servers OS, Oracle database and Unix provide advanced audit management features so that only relevant events and activities viz., privileged user activity, changes to master are logged.

In addition to enabling the audit logs in systems, there should be a process in place to periodically review audit logs to detect any unauthorized events, activities and exceptions. Typically, audit logs should be generated and reviewed by someone independent of the IT function or those having privileged user access.

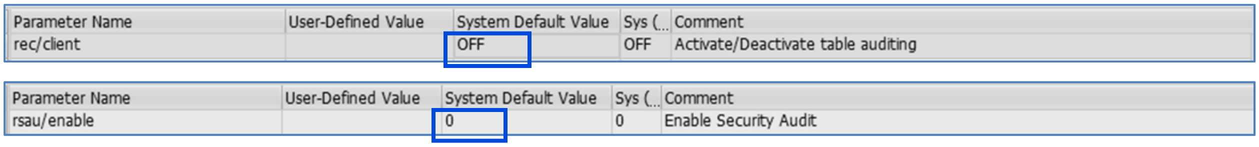
Example of audit log configuration in Windows Server. In this example, audit logs are set as Not Defined i.e., auditing is not enabled



Policy	Policy Setting
Audit account logon events	Not Defined
Audit account management	Not Defined
Audit directory service access	Not Defined
Audit logon events	Not Defined
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

Fig 2.9.2: Audit log configuration

Example of shows configuration to enable table logs and security logs in ERP. OFF indicates table log are not enabled, 0 indicates security logs are not enabled.



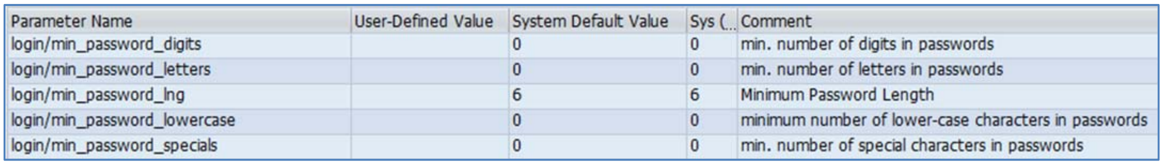
Parameter Name	User-Defined Value	System Default Value	Sys (...	Comment
rec/client		OFF	OFF	Activate/Deactivate table auditing

Parameter Name	User-Defined Value	System Default Value	Sys (...	Comment
rsau/enable		0	0	Enable Security Audit

Fig 2.9.3: Security Logs in ERP

- **Password configuration**: a password is a secret code that is used in combination with a user id to gain access into an IT system or application. Because of the sensitive nature of a password, unauthorised users including hackers most often target the passwords of users, specifically privileged users. Most systems provide the options for configuring the security and strength of passwords in order to protect being compromised from attacks. Password configuration and controls are applicable for all layers of access security.

  Example of a password configuration in ERP as shown in Fig 2.9.4.



Parameter Name	User-Defined Value	System Default Value	Sys (...	Comment
login/min_password_digits		0	0	min. number of digits in passwords
login/min_password_letters		0	0	min. number of letters in passwords
login/min_password_lng		6	6	Minimum Password Length
login/min_password_lowercase		0	0	minimum number of lower-case characters in passwords
login/min_password_specials		0	0	min. number of special characters in passwords

Fig 2.9.4: Password configuration in ERP

All new systems, applications and network equipment are supplied with one or more pre-created user ids, commonly known as "default users", including the administration user id. The purpose of these default users is to facilitate easy installation and implementation of the respective software. However, the risk with default users is they are supplied with a password (known as "default password") that is published openly and known to all. The default passwords should be changed immediately after installation but many companies forget to change the default passwords which can be misused by an unauthorized user or hacker.

Example of default users and corresponding default passwords in an oracle database.

User ID	**Password**	**Password hash value**
ORACLE	ORACLE	38E38619A12E0257
ORADBA	ORADBAPASS	C37E732953A8ABDB
DBSNMP	DBSNMP	E066D214D5421CCC
DEMO	DEMO	4646116A123897CF
ADMIN	JETSPEED	CAC22318F162D597
ADMINISTRATOR	ADMIN	F9ED601D936158BD
APPLSYS	APPLSYS	FE84888987A6BF5A
SYSTEM	CHANGE_ON_INSTALL	8BF0DA8E551DE1B9
SYS	0RACLE8	1FA22316B703EBDD
OUTLN	OUTLN	4A3BA55E08595C81
SAPR3	SAP	58872B4319A76363
SCOTT	TIGER	F894844C34402B67
SYSADM	SYSADM	BA3E855E93B5B9B0

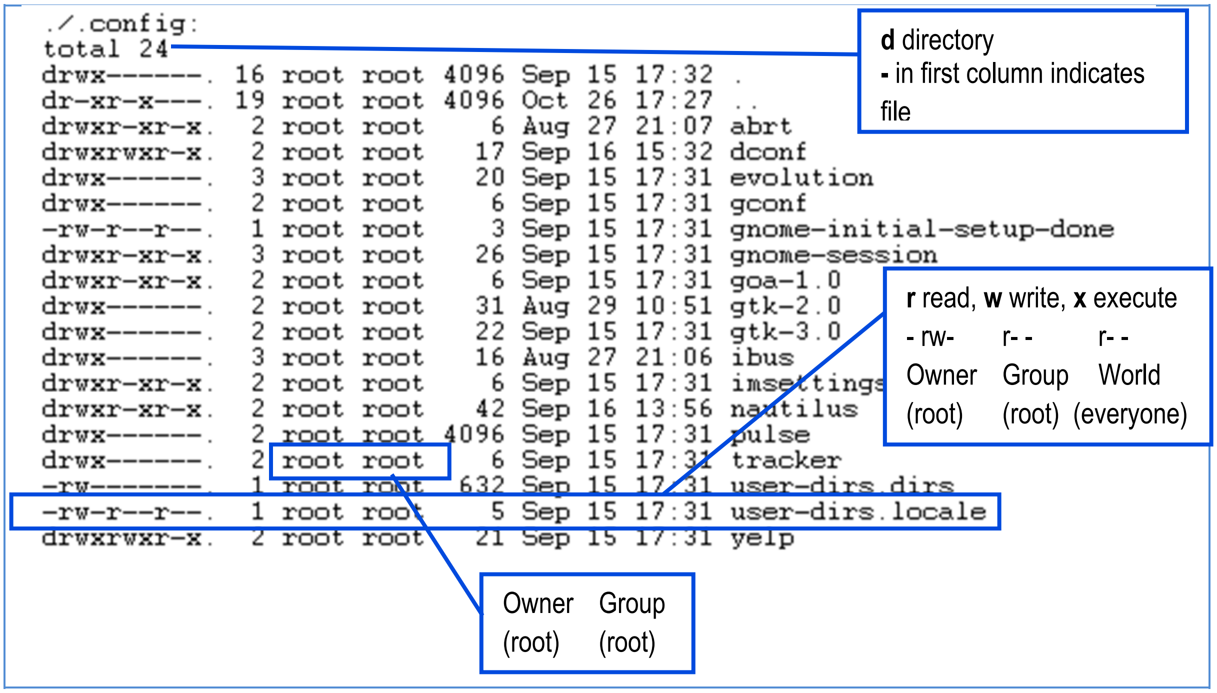
Table 3: Default password in Oracle

- **Direct data access**: all data including financial data, master data, transaction data and user data is stored in a database, logically represented as rows and columns (similar to an excel spreadsheet). Some common databases include Oracle 12g, MS-SQL Server 2012 and MySQL. The data is physically stored in the form of data files located in the operating system. Direct data access is relevant at the database and operating system layers of access security.

It is possible to directly access and modify/ manipulate data in a database using tools viz., SQL Plus, Toad, SQL Navigator, Enterprise Database Management tools. Direct data access is high risk because it bypasses security and business controls defined at the application layer. Normally only a limited number of users are likely to have database access including database administrators and IT operations personnel.

- **File system security**: application programs, data files, backups, configuration and user security files, etc are physically stored in the form of files and directories/folders in the operating system. An operating system is a system software that converts high level user command to machine language. Examples of operating systems include Windows 10 (desktop), Windows 2012 Server, Unix (HP-UX, AIX) and Linux (RHEL, SuSE, Ubuntu). Access to the critical files and directories that contain sensitive information should be restricted to a limited number of users including systems administrators and IT operations personnel. File system security is relevant at the operating system layer of access security.

  Example of file system permissions in UNIX as shown in Fig 2.9.5.



```
./.config:
total 24
drwx------. 16 root root 4096 Sep 15 17:32 .
dr-xr-x---. 19 root root 4096 Oct 26 17:27 ..
drwxr-xr-x.  2 root root    6 Aug 27 21:07 abrt
drwxrwxr-x.  2 root root   17 Sep 16 15:32 dconf
drwx------.  3 root root   20 Sep 15 17:31 evolution
drwx------.  2 root root    6 Sep 15 17:31 gconf
-rw-r--r--.  1 root root    3 Sep 15 17:31 gnome-initial-setup-done
drwxr-xr-x.  3 root root   26 Sep 15 17:31 gnome-session
drwxr-xr-x.  2 root root    6 Sep 15 17:31 goa-1.0
drwx------.  2 root root   31 Aug 29 10:51 gtk-2.0
drwx------.  2 root root   22 Sep 15 17:31 gtk-3.0
drwx------.  3 root root   16 Aug 27 21:06 ibus
drwxr-xr-x.  2 root root    6 Sep 15 17:31 imsettings
drwxr-xr-x.  2 root root   42 Sep 16 13:56 nautilus
drwx------.  2 root root 4096 Sep 15 17:31 pulse
drwx------.  2 root root    6 Sep 15 17:31 tracker
-rw-------.  1 root root  632 Sep 15 17:31 user-dirs.dirs
-rw-r--r--.  1 root root    5 Sep 15 17:31 user-dirs.locale
drwxrwxr-x.  2 root root   21 Sep 15 17:31 yelp
```

d directory
- in first column indicates file

r read, **w** write, **x** execute
- rw- r- - r- -
Owner (root) Group (root) World (everyone)

Owner (root) Group (root)

Fig 2.9.5: File system permission in UNIX

- **Domain security**: a domain is a central repository of objects including users, groups, and access rights and permissions implemented in a server operating system viz., Windows 2012 Server. A domain forms part of a company's internal network and is used to for the authentication and authorisation of users before they can access applications and network resources viz., shared drives, folders and files.

- **Firewall, VPN, Anti-virus/malware**: IT systems operate in a networked environment in which several systems and devices are connected and communicate with each other and exchange data using ports, services and network protocols. Firewalls are installed and configured at the perimeter network layer to protect the company's IT systems from external threats and remote attacks. Virtual Private Network (VPN) allows users to remotely access to a company IT systems and applications using a secure and encrypted channel through a public network like the internet. Anti-virus and anti-malware software is used to protect data corruption that are caused by computer viruses.

  Example of a remote access through external network, firewall, and internal network as shown in Fig 2.9.6

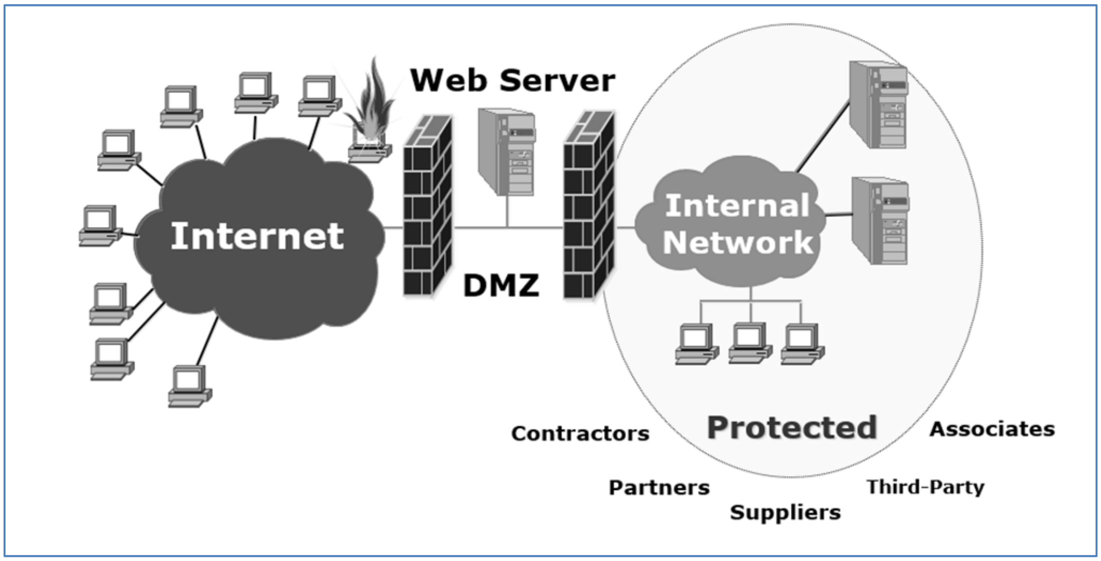


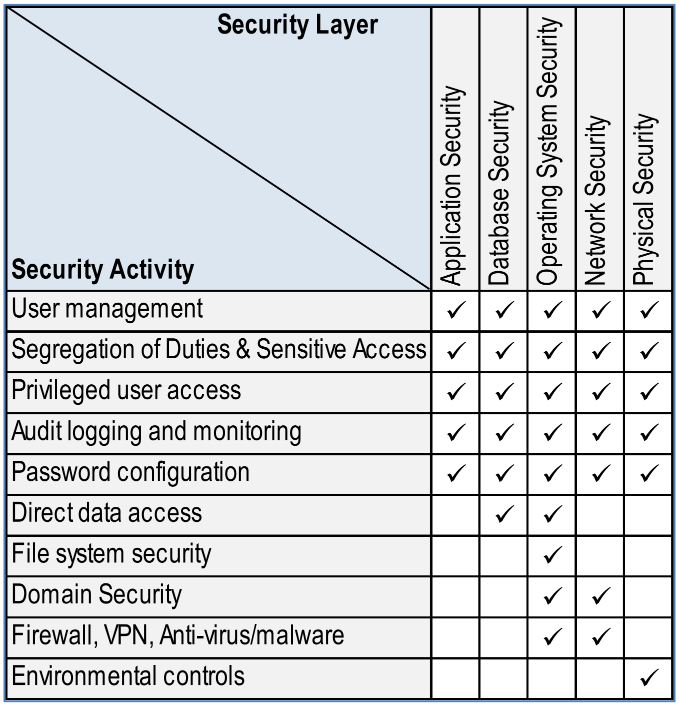
Fig 2.9.6: remote access through external network, firewall, and internal network

- **Environmental controls**: environmental controls form part of the physical security layer of access security. Computing facilities that process, store, and transmit sensitive and critical data require protection from environmental hazards viz., fire, water, dust, humidity and heat that could result in system failures, data corruption and loss of data. Smoke detectors, fire extinguisher, air conditioning, temperature and humidity control, raised flooring are implemented to protect systems from environmental controls.

The manner in which access security is implemented will vary based on the nature, size and complexity of business operations and the extent to which IT systems are used. While most of the activities mentioned above are critical for the company, it is likely that some of these activities are less relevant to an audit of financial statements.

For example, security activities at the database and application layer that directly protect the integrity of financial data will be more relevant to audit. Whereas, the security activities at the outer layers of network and physical layers would be less relevant to audit. The auditor should determine the relevant activities and controls based on risk assessment.

The illustration below summarises the relevance of the various access security activities to the layers of security.



Security Layer Security Activity	Application Security	Database Security	Operating System Security	Network Security	Physical Security
User management	✓	✓	✓	✓	✓
Segregation of Duties & Sensitive Access	✓	✓	✓	✓	✓
Privileged user access	✓	✓	✓	✓	✓
Audit logging and monitoring	✓	✓	✓	✓	✓
Password configuration	✓	✓	✓	✓	✓
Direct data access		✓	✓		
File system security			✓		
Domain Security			✓	✓	
Firewall, VPN, Anti-virus/malware			✓	✓	
Environmental controls					✓

Fig 2.9.7: Various access security activities

The table below has examples of risk and controls that an auditor may consider when reviewing access security

Ref No.	Activity	Risk	Control description
1	User management	Unauthorised access to systems	There is a formal approval process of creating, changing and removing all access to the application.
2	User management	Users have excessive access to systems	There is a process of periodic reviews to verify that user access is consistent with job responsibilities.
3	Password Configuration	Weak passwords may compromise security controls.	A robust password policy is implemented at the application level, database and operating system.
4	Access logging and monitoring	Unauthorised activities may go undetected.	Special system utilities for accessing data are logged and reviewed on a regular basis.
5	Access logging and monitoring	Unauthorised activities may go undetected.	Audit trail controls are designed and monitored by the management for potential unauthorized activities.

Ref No.	Activity	Risk	Control description
6	Network security	Computer virus may cause data loss and corruption	Appropriate software is installed, updated regularly to protect the system from virus attacks.
7	Perimeter network security	Unauthorised persons and hackers may gain access to financial data remotely.	The internal network is protected from unauthorized access via external network connections (i.e. internet) by appropriate placements of firewalls, etc.
8	Physical security	Unauthorised users may gain access to computing facilities and data	Physical access to computer facilities, data centres, and removable storage media is appropriately restricted.

Table 4

2.10 Procedures for Review of Data Center and Network Operations

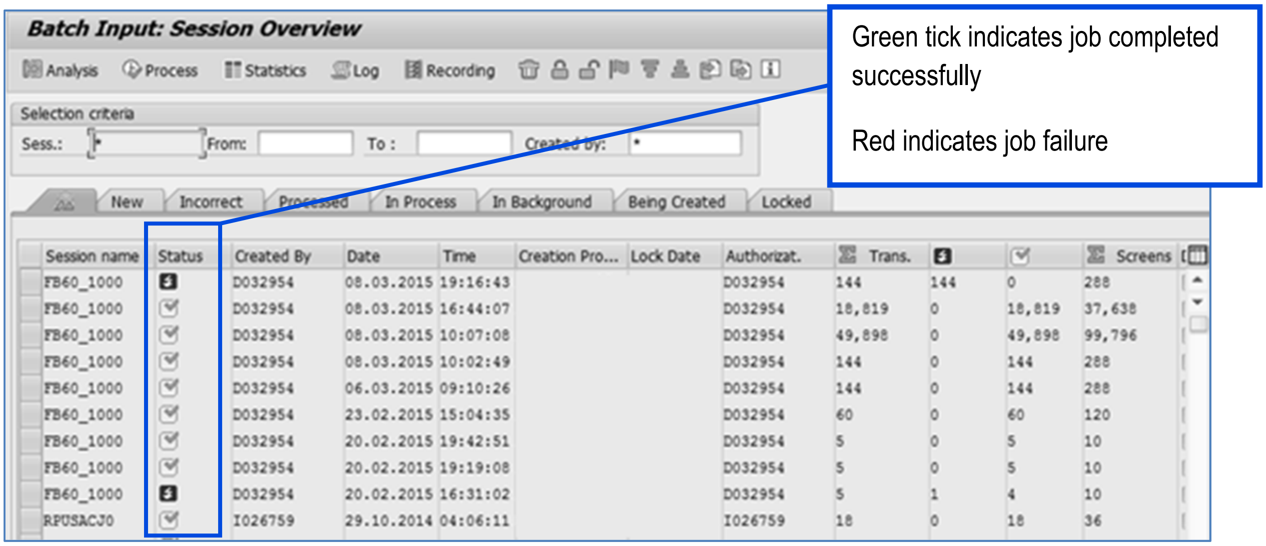
Data centre and network operations, also known as computer operations, is one of the categories or domain of General IT Controls that involves the understanding and evaluating the process, risks and controls that are relevant to day-to-day operations carried out in the IT environment.

The objective of data center and network operations is "To ensure that production systems are processed to meet financial reporting objectives". The various activities in this domain include the following

- **Batch jobs**: processing of batch jobs involves combining several transactions of the same nature for processing at the same time. Typically, batch jobs are designed to execute automatically at a pre-scheduled time without user intervention. A user could also initiate a batch job and schedule it for execution at a particular point of time.

  For example, all the purchase invoices are processed overnight by a batch job which is scheduled to execute at midnight daily so that the payment can be made next day. Another common example is of a batch job is a discount calculation program that is manually executed by a user at the end of every month to process discounts to dealers.

  Example of monitoring batch jobs in ERP as shown in Fig 2.10.1.



Selection criteria

Sess.: * From: To : Created by: *

Session name	Status	Created By	Date	Time	Creation Pro...	Lock Date	Authorizat.	Trans.	☒	☑	Screens
FB60_1000	☒	D032954	08.03.2015	19:16:43			D032954	144	144	0	288
FB60_1000	☑	D032954	08.03.2015	16:44:07			D032954	18,819	0	18,819	37,638
FB60_1000	☑	D032954	08.03.2015	10:07:08			D032954	49,898	0	49,898	99,796
FB60_1000	☑	D032954	08.03.2015	10:02:49			D032954	144	0	144	288
FB60_1000	☑	D032954	06.03.2015	09:10:26			D032954	144	0	144	288
FB60_1000	☑	D032954	23.02.2015	15:04:35			D032954	60	0	60	120
FB60_1000	☑	D032954	20.02.2015	19:42:51			D032954	5	0	5	10
FB60_1000	☑	D032954	20.02.2015	19:19:08			D032954	5	0	5	10
FB60_1000	☒	D032954	20.02.2015	16:31:02			D032954	5	1	4	10
RPUSACJ0	☑	I026759	29.10.2014	04:06:11			I026759	18	0	18	36

Green tick indicates job completed successfully

Red indicates job failure

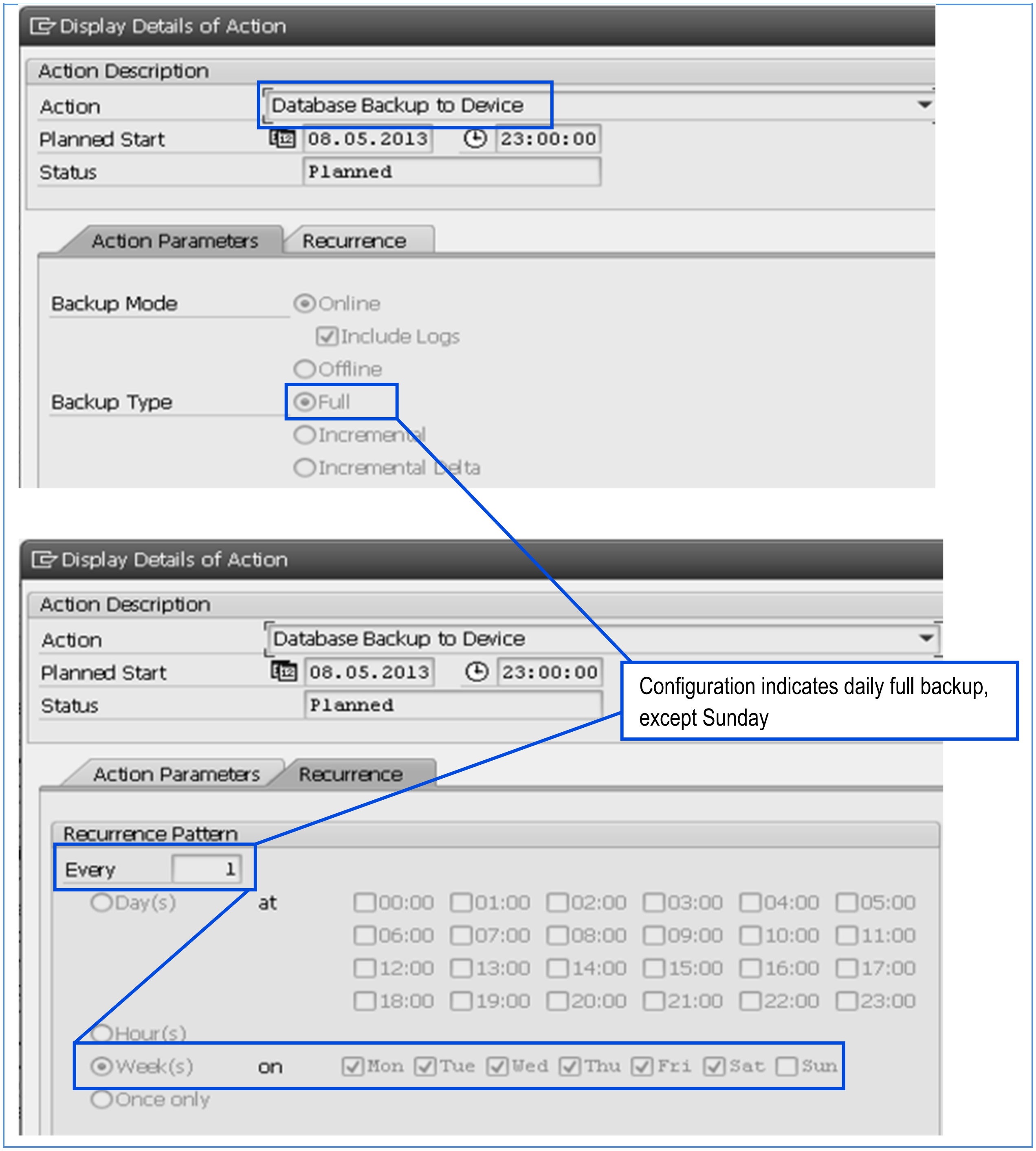
Fig 2.10.1: Batch jobs in ERP

- **Real-time processing**: in a real-time processing system, transactions are initiated, processed and recorded immediately as and when they occur, without delay.

  For example, when a sales invoice is created in a ERP, the corresponding accounting entries are automatically posted to the respective sub-ledgers and general ledgers at the same time account balances are updated immediately.

- **Data Backups**: backup involves making periodic copies of existing data and applications to an alternate storage media which can be useful for recovery in the event of data loss or corruption of data. The content, frequency, storage, retention and restoration of backups depend on the nature of business and criticality of data.

  For example, the data in a ERP system of a cement manufacturing company is copied every day to an external drive. Once a week an additional copy of the data is copied to a tape and stored in a remote branch office in a fire proof safe. On the other hand, the data of a financial services company may be copied to an external system in real-time using database mirroring and replication techniques i.e., two copies of the same database are maintained at different locations and every transaction is automatically copied on to both the databases to ensure high availability of systems. Example of backup schedule in ERP.



Display Details of Action

Action Description

Action: Database Backup to Device

Planned Start: 08.05.2013 23:00:00

Status: Planned

Action Parameters | Recurrence

Backup Mode: ● Online

☑ Include Logs

○ Offline

Backup Type: ● Full

○ Incremental

○ Incremental Delta

Display Details of Action

Action Description

Action: Database Backup to Device

Planned Start: 08.05.2013 23:00:00

Status: Planned

Action Parameters | Recurrence

Recurrence Pattern

Every 1

○ Day(s) at □00:00 □01:00 □02:00 □03:00 □04:00 □05:00
□06:00 □07:00 □08:00 □09:00 □10:00 □11:00
□12:00 □13:00 □14:00 □15:00 □16:00 □17:00
□18:00 □19:00 □20:00 □21:00 □22:00 □23:00

○ Hour(s)

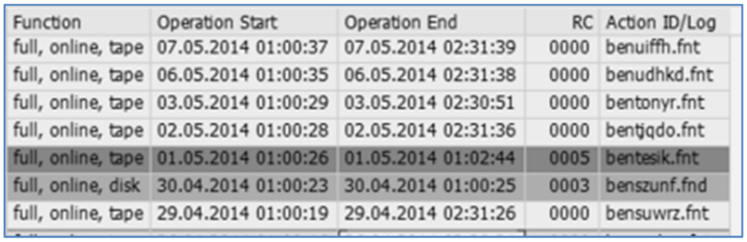
● Week(s) on ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat □ Sun

○ Once only

Configuration indicates daily full backup, except Sunday

Fig 2.10.2: Backup Data in ERP

Example of backup log, return code RC 0000 indicates successful completion of backup, RC 0005 and 0003 indicate error in backup.



Function	Operation Start	Operation End	RC	Action ID/Log
full, online, tape	07.05.2014 01:00:37	07.05.2014 02:31:39	0000	benuiffh.fnt
full, online, tape	06.05.2014 01:00:35	06.05.2014 02:31:38	0000	benudhkd.fnt
full, online, tape	03.05.2014 01:00:29	03.05.2014 02:30:51	0000	bentonyr.fnt
full, online, tape	02.05.2014 01:00:28	02.05.2014 02:31:36	0000	bentjqdo.fnt
full, online, tape	01.05.2014 01:00:26	01.05.2014 01:02:44	0005	bentesik.fnt
full, online, disk	30.04.2014 01:00:23	30.04.2014 01:00:25	0003	benszunf.fnd
full, online, tape	29.04.2014 01:00:19	29.04.2014 02:31:26	0000	bensuwrz.fnt

Fig 2.10.3: Backup & return Code

- **Interfaces between systems**: data flows between two or more IT systems is known as an interface. The flow of data could be real-time, scheduled using batch jobs or manual. In case a company is using only a single ERP system, interfaces may not be relevant.

  For example, consider a software services company that has in-house application for Projects, PeopleSoft for HR & Payroll and Oracle EBS for accounting and financial reporting. At month end, invoicing is done in Oracle EBS based on the project status and rates obtained from the Projects application, staff information and timesheets from PeopleSoft. The data flow between the three systems happens through interfaces. On the other hand, consider a mid-sized manufacturing company using an Oracle EBS application for all business transactions. In this example, there are no interfaces because there is only one system.

- **Recovery from Failures**: In the event of failures that impacts the availability of IT systems the company should be able to cope with and recover from the system failures. A business continuity plan is a document that details the risks, business impact analysis and other procedures to help a company in going on with business transactions when failures occur. Disaster recovery plan, which is a part of the larger business continuity plan, focuses on the procedures for restoring the IT systems back to normal state after the failure.

  For example, a telecom company installs multiple backup power systems including diesel generators at tower sites to keep the network operational in the event of power outages. Core banking systems, railway/airline ticketing systems, e-commerce portals, etc., have an operational secondary data center located at a remote site that would allow the bank to continue operations in the event of failure of the primary data center.

- **IT Helpdesk**: a helpdesk is a facility to address and resolve user requests including queries, incidents and problems related to IT systems and applications. Typically, all requests are logged and monitored to minimize disruption to business.

  For example, a mid-sized consumer retail company with several outlets across a city has a central IT helpdesk to resolve user requests. All requests are recorded in an online intranet portal and there is also a toll-free number which users can make use of to log service requests. Requests have to be resolved in a timely manner based on the priority and severity recorded and governed by service level agreements between IT department and business.

The activities in this domain are mainly to ensure that IT systems are available for carrying on business transactions and to detect and correct disruptions to IT systems and applications. All activities in computer operations may not be relevant to an audit of financial statements being operational in nature.

For example, service level agreements are put in place to ensure that systems are available for users to process transactions, similarly a IT helpdesk provides support to users so they can continue using systems for transactions. While the service level agreements and helpdesk are important activities for ensuring availability of systems for business, there is no direct impact on the financial transactions and reporting aspects.

However, activities viz., batch jobs, interfaces and backups could directly impact the integrity of financial transactions and data and hence considered relevant for audit.

The table below has examples of risk and controls that an auditor may consider when reviewing computer operations.

Ref No.	Activity	Risk	Control description
1	Batch scheduling and processing	Unauthorized changes are made to batch jobs.	Additions, changes and deletion to job schedules are documented and authorized.
2	Batch scheduling and processing	Failures in execution of batch job.	All batch jobs are monitored for successful completion. Any errors and incomplete jobs are identified and rectified in a timely manner.
3	Real-time processing	Unauthorised changes are made to the configuration of real-time components.	There exists a consistent procedure for making changes to the configuration of real-time processing components (including middleware, where applicable).
4	Backup and Recovery	Loss of critical data due to data corruption system failures.	Formal backup policy exists, is implemented and duly monitored for compliance.
5	Backup and Recovery	Loss of critical data due to fire and theft	On site and Off-site backups are maintained securely.
6	Backup and Recovery	Backup is incomplete or corruption of backup media	Back up recovery is periodically tested to ensure that it works when required.
7	Interfaces between systems	Data transfer between systems is incomplete or inaccurate	Plans for the business continuity is kept up to date and tested.
8	Disaster recovery	Data recovery plan is obsolete	Disaster recovery plans are updated once a year and tested two times a year.

Table 5

2.11 Procedures for Review of Application System Acquisition, Development and Maintenance

The application system acquisition, development and maintenance, also called program development, is one of the categories or domain of General IT Controls that involves the understanding and evaluating the process, risks and controls that are relevant to a company when major changes occur in the IT environment. For example,

- New IT systems and applications are acquired and implemented in the company
- Existing IT systems are migrated to a different system
- Major changes occur in IT applications or infrastructure

The objective of application system acquisition, development and maintenance is “To ensure that systems are developed, configured and implemented to meet financial reporting objectives”. The various activities in this domain include the following

- Project Planning
- Analysis & Design
- Data Conversion/Development
- Testing
- Go-Live Decision
- Documentation & Training

In activities mentioned above represent the System Development Life Cycle (SDLC) in software development terminology which is one of the most common method that is followed for development and implementation of new systems and applications including ERP systems.

The auditor should consider this domain of General IT Controls to be relevant for audit only when major changes occur in the IT environment that impact the financial reporting. For example, if a company is implementing a new ERP system to automate the business process of sales, purchase, inventory, payroll and general ledger, the auditor should consider reviewing process and controls in this domain because this change impacts the financial reporting. On the other hand, if a company is implementing a new customer relationship management (CRM) system for improving marketing and customer service, the auditor may not consider reviewing this implementation because there is no impact on financial reporting.

The audit approach, methods and review procedures that and auditor should consider have been provided in more detail in the chapter on **“New System and Data Migration Review”**

2.12 Concluding on Impact of Deficiencies in GITCS on Audit

During a review of General IT Controls, deficiencies in design and operating effectiveness may be observed. Examples of deficiencies in GITCs include:

(a) password controls are not enabled

(b) a formal sign-off for user acceptance testing has not been obtained for program changes

(c) errors and batch jobs have not been resolved

(d) privileged user access has been granted to unauthorised users

(e) direct-data changes have been made in database without approvals

(f) audit logs have not been enabled

Having found deficiencies, the auditor should evaluate the impact of these deficiencies on the audit. For this evaluation, the auditor should consider the following:

- which automated controls, IT dependent controls and reports/IPE will be impacted
- are there compensating controls that mitigate the risk, can we test the compensating controls. For example, are there manual checks and controls that mitigate risk of material misstatement.
- is there evidence that deficiency was not exploited. For example, even though privileged user access was granted to unauthorised users, have the users used this level of access (it is possible the users may not be even aware they had the access)
- consider data analytics using CAATs to verify the integrity of account balances. For example, the auditor can extract transaction data from the ERP system and use ACL to independently reconcile sub-ledger with general ledger balance.
- determine the aggregate financial impact of the deficiencies and compare with materiality.

The above examples are some of the ways in which the auditor evaluates the deficiencies to assess impact on audit. Wherever necessary, the auditor should consider revising the planned audit response by altering the nature, timing and extent of audit procedures, including controls testing and substantive testing, to address the risk of material misstatement in financial statements. For example, the auditor may increase the sample sizes for controls testing or test reports and IPE substantively.

Evaluation and assessment of deficiencies requires the auditor to apply professional judgement and the auditor is required, as per SA 230, to explicitly document the process of evaluation, factors considered, additional audit evidence obtained and conclusions reached to support the audit opinion.

2.13 When to Test GITCS

Understanding of the ERP environment is obtained during the planning phase of an audit of financial statements. The timing for testing General IT Controls in an ERP environment will vary depending on several factors including the following:

- Effectiveness of the Entity Level Controls
- Understanding of Business process and controls
- Level of automation in business process
- Dependencies on IT i.e., IPE/Reports, IT Dependent controls
- Risk assessment, including IT risks
- IT systems and application in scope

- Outsourced IT activities
- Deficiencies observed in past audits
- New systems and changes in existing IT environment

The above are some of the factors that the auditor should consider in determining the timing of General IT Controls. In a typical ERP environment, it is more likely that the testing for GITCs is performed early in the audit process, close to the planning stage, because of the dependencies that other audit work, including controls and substantive testing, have on effectiveness of GITCs.

In deciding the timing for GITCs tests, the auditor should also factor the possibility of finding deficiencies and the time required for remediation and re-testing GITCs. In other words, if the GITCs are tested during the planning phase of audit, there will be sufficient time to rectify any exceptions and deficiencies and re-test or plan alternate audit procedures prior to balance sheet date. On the other hand, if the GITCs are tested closer to year-end, there may not be sufficient time to rectify deficiencies or carry out alternate audit procedures.

2.14 Exercises

Multiple Choice Questions

1. What are data flows between multiple IT systems also known as,

   (a) Batch jobs

   (b) Interfaces

   (c) Databases

   (d) Operating systems

2. Which of the following activity from the Data center and network operations domain of GITCs is less likely to have an impact on audit,

   (a) Service Level Agreements

   (b) Data backups

   (c) Real-time processing

   (d) All of the above

3 What is the risk due to default passwords,

   (a) They are easy to guess

   (b) Openly know

   (c) Do not comply with company's password policy

   (d) All of the above

4. Privileged users are more commonly known as,

   (a) Business users

(b) Normal users

(c) Super users

(d) End users

5. Segregation of duties is applicable to which layer of access security,

(a) Application security

(b) Database security

(c) Network security

(d) All of the above

Fill in the blanks

6. With respect to samples selected for testing, the auditor is required to document _________ for sample size and how the auditor ensured ______
7. The software methodology used for carrying out program development and program changes is known as ______________
8. Deficiencies in GITCs will impact the ________ of automated controls, IT-dependent controls and IPEs
9. ____________ is considered high risk because it bypasses the application controls and could compromise data integrity.
10. A _________ contains procedures for restoring the IT systems back to normal state after a failure.

True or False

11. The auditor should review GITCs for all IT systems and applications used at a company (True/False)
12. Developers and programmers should not be given access to production environment (True/False)
13. It is more efficient to test GITCs at year-end (True/False)
14. Batch jobs should be monitored for failures so that corrective action can be taken (True/False)
15. Environmental controls are applicable to all layers of access security (True/False)

2.15 Case study

Access Ltd. is using an ERP which has Sales, Purchase, Inventory and GL modules. The ERP has standard reports for P&L account, Balance Sheet, Cash Flow statement. However, the Finance Controller wanted three new reports with a different presentation and format which were created and implemented during the year under audit.

You have been a member of the audit team for the last three years. For the current year, in the initial meetings with the client, you are informed that the company has developed these three new reports. From the audit of the previous years you are aware that the General IT Controls at the company are effective.

You have started the GITCs review for the current year. Your task is to,

(a) Identify which domains of GITCs will be applicable

(b) Document three risks and relevant controls you plan to test to validate whether the reports have been prepared in a controlled manner.

2.16 Glossary

ACL	Audit Command Language (CAAT Tool)
AIX	Unix Operating System for IBM servers
BCP	Business Continuity Plan
CAATs	Computer Assisted Audit Techniques
CR	Change Request
CRM	Customer Relationship Management (application software)
DB	Data Base
DMZ	De-Militarized Zone
DR	Disaster Recovery
ELC	Entity Level Controls
ERP	Enterprise Resource Planning (application software)
GITC	General Information Technology Controls
HOD	Head of Department
HP-UX	Unix Operating System for HP servers
HR	Human Resource
IPE	Information Produced by Entity (reports, etc)
IT	Information Technology
LAN	Local Area Network
Oracle EBS	Enterprise Business Suite, ERP application software provided by Oracle Corporation
OS	Operating System
RHEL	Red Hat Enterprise Linux, a type of Linux Operating System
SA	Standards on Auditing
SA/SOD	Sensitive Access / Segregation of Duties
SAP	Systems, Applications and Products in data processing, ERP application software
SDLC	System Development Life Cycle, a software development methodology
SQL	Structured Query Language, high-level software language for database systems
SuSE	A type of Linux Operating System
UAT	User Acceptance Testing
VPN	Virtual Private Network
WAN	Wide Area Network

2.17 References and Further Reading

1. Standards on Auditing published by the Institute of Chartered Accountants of India (ICAI), www.icai.org > Resources
2. Guidance Note on Audit of Internal Financial Controls Over Financial Reporting issued by Auditing and Assurance Standards Board. - (14-09-2015), www.icai.org
3. Companies Act 2013, www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf

2.18 Answers to Excises

1. Correct answer is B

   Interfaces are data flows between two or more systems in an IT environment
2. Correct answer is A

   Service level agreements are operational controls put in place to ensure availability and quality of IT services and hence less likely to impact the financial reporting aspects.

   Backups and Real-time processing are more likely to be relevant because there is a risk of data loss and data corruption due to system failures.
3. Correct answer is D

   All three risks mentioned are relevant.
4. Correct answer is C

   Privileged users are also known as super users or administrators and have unrestricted access to systems.

   Business users, normal users and end users refer to the same type of users who have restricted access to systems.
5. Correct answer is D

   Segregation of Duties is pervasive and applicable to all layers of access security
6. Justification, Completeness of population
7. Systems Development Life Cycle or SDLC
8. Reliability
9. Direct data access
10. Disaster Recovery Plan or DR Plan
11. False

    The auditor is required to review GITCs for relevant IT systems that impact financial reporting objectives.
12. True

    Developers and programmer access should be restricted to development environment and test environment

13. False

    Timing for a review of GITCs depends on several factors and could vary based on the outcome of these factors. However, in an ERP environment testing for GITCs is normally performed early in the audit process, close to the planning stage, because other audit work depends on the effectiveness of GITCs.

14. True

    Errors or failures in Batch jobs could impact the completeness and accuracy of financial transactions and hence batch jobs should be monitored, any errors and failures should be rectified in a timely manner.

15. False

    Environmental controls are applicable to the physical security layer of access security.

2.19 Answer to Case Study

(a) The GITC domains that will be applicable are Program Changes and Access Security.

(b) Relevant risks and controls are as follows:

Ref No.	Activity	Risk	Control description
1	Change Request	Unauthorised changes are processed	The change request is approved by the department In-charge or Head of department (HOD). Changes to IT infrastructure components are approved by IT Head.
2	Testing	Untested changes could compromise the integrity of financial data	Unit testing is performed by developer, user acceptance testing is done by end user prior to implementing in production environment.
3	Segregation of duties	Changes are made directly in production environment and may result in loss of data and program integrity.	Three separate environments exist for development, quality (test) and production. Separate teams are involved in development and migration of changes to production. Development of changes are done by consultants and movement of changes to production is performed by System Administration only after approval.
4	Implementation	Changes are implemented by unauthorised persons.	Access to migrate changes to production is restricted to System Administrators only.

CHAPTER 3

AUTOMATED APPLICATION CONTROLS

LEARNING OBJECTIVES

- To understand what are Automated Application Controls
- To understand the types of Automated Application Controls
- To understand the Various Business Cycles, Obtain Process Understanding and Identification of Controls
- To understand the procedures for review of Design Effectiveness and Operating Effectiveness of Application Controls
- To understand when to test Automated Application Controls
- To understand what sample size to follow for testing Automated Application Controls
- To analyse and conclude on impact of deficiencies in Automated Application Controls on audit

3.1 Overview

Clause (i) of Sub-section 3 of Section 143 of the Companies Act 2013, requires the auditors' report to state whether the company has adequate internal financial controls system in place and the operating effectiveness of such controls.

In June 2003, the Securities and Exchange Commission (SEC) of the United States of America adopted Rules for the implementation of Sarbanes – Oxley Act, 2002 (SOX) that required certification of the Internal Controls over Financial Reporting (ICFR) by the management and by the auditors.

There are other regulatory requirements such as J-Sox etc. where auditors are required to certify the adequacy of internal controls as implemented by Management.

Thus, the auditors are required to express an opinion on the effectiveness of an company's internal controls over financial reporting and such opinion is in addition to and distinct from the opinion expressed by the auditor on the financial statements.

As mentioned in the Introduction Chapter, SA 315 talks about identifying the risk of material misstatement through understanding of the Company and its environment. The company implements an internal control framework to minimise the risk. The auditor shall understand the internal controls within the company. While understanding the internal controls, the auditor will understand the types in internal controls as implemented by the company. Internal controls are implemented by a company irrespective of whether they have implemented an ERP or not. In this session, we shall try to understand the implementation of internal controls in an ERP environment.

Some reasons why ERP's are implemented by companies are:

- To move from manual processes to automated processes and achieve better operational efficiencies
- To achieve ease of reporting due to high level of sophistication of the reports defined in ERP's
- To have a better internal control environment as ERP's allow for processes and controls to be automated
- To respond faster to competition and the outside business environment.

While there are advantages and efficiencies that can be gained by automation, there is also a heightened risk of processes and controls being compromised within the ERP. Hence, it is important for the company to implement controls within the ERP. Such controls are called as **Automated Application Controls (AACs)**. These controls are implemented over the processing of transactions and data within the application. They are specific to each application. Hence, they are called **AACs**. In this chapter, we shall understand the AACs and get to know some examples.

The Guidance Note on Internal Financial Controls over Financial Reporting defines "*Application controls as those controls that achieve the business objectives of timely, accurate and reliable information."* The application controls that are automated within the ERP are called AACs.

The Committee of the Sponsoring Organisations of the Treadway Commission (COSO) defines controls activities "*as the policies and procedures that help management objectives are carried out."* Thus, AACs are those policies, procedures and activities designed to provide reasonable assurance that objectives relevant to a given automated solution are achieved.

Another explanation is AACs are controls that prevents applications from executing unauthorised transactions in a manner that puts data at risk.

The objectives of AACs are to ensure

- completeness of data
- accuracy of data
- the validity of the transactions
- only authorised transactions are processed
- appropriate segregation of duties.

This is also mentioned in IG 7.5 in The Guidance Note on Internal Financial Controls over Financial Reporting

Some of the risks that are addressed by such AAC's are:

- Risk of unauthorised personnel entering the data
- Risk of personnel entering unauthorised data
- Risk of inaccurate processing of data
- Risk of unauthorised changes / modifications to data
- Risk of data being obtained by unauthorised personnel

3.2 Types of Automated Application Controls

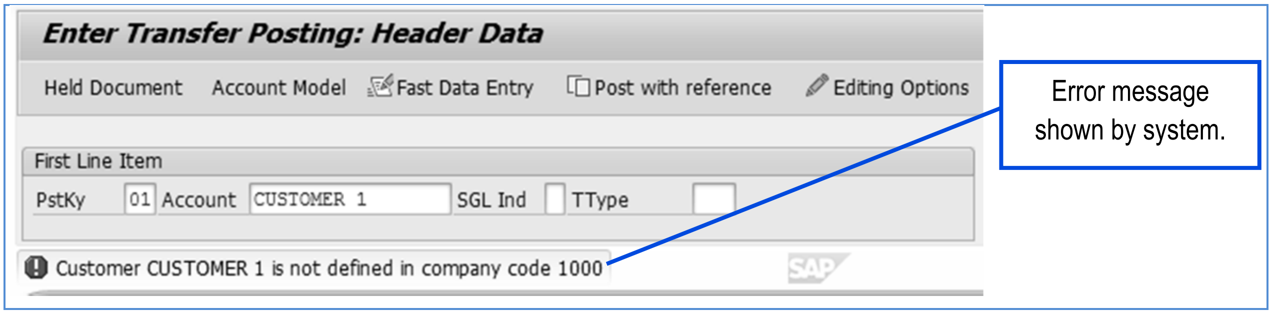
Some of the different types of Automated Application Controls to address the above mentioned risks are:

1. **Inherent controls** – These controls come along with the implemented ERP. These can also be called Input controls. These are some basic controls such as

   (i) Debit = Credit. All transactions should match

   (ii) Validation checks - Fields where numbers are entered, will not accept alpha numeric or alphabets etc.

   Error message while entering account number which is not defined in chart of accounts:



Enter Transfer Posting: Header Data

PstKy 01 Account CUSTOMER 1

Customer CUSTOMER 1 is not defined in company code 1000

Error message shown by system.

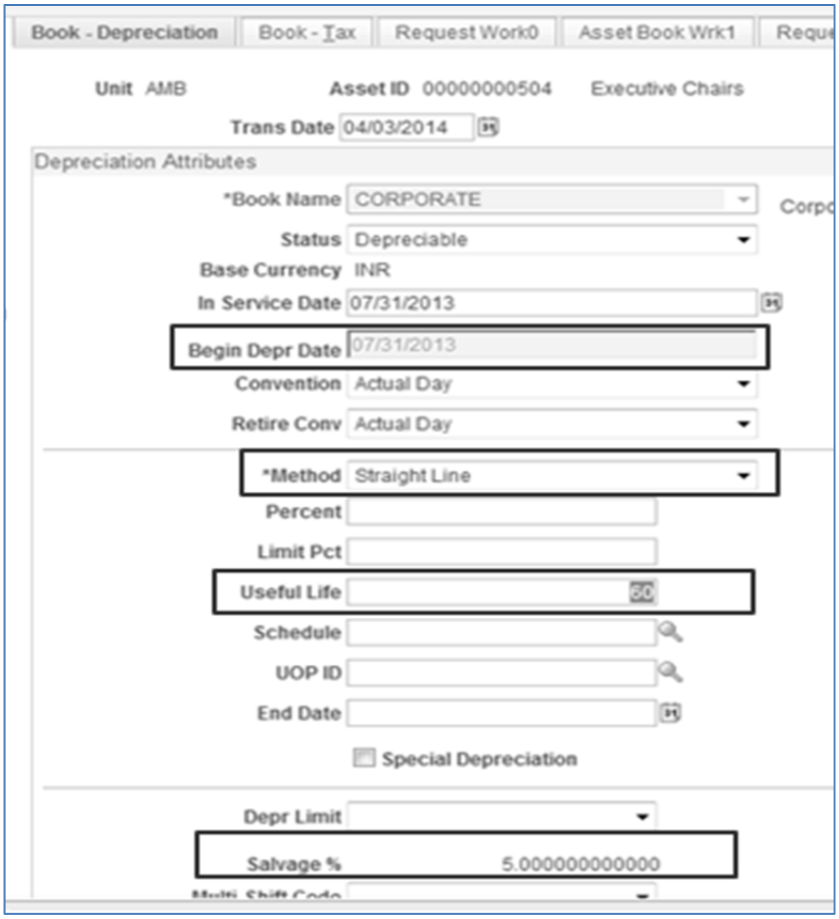
Fig 3.2.1: Error message

   (iii) Duplicate check – When a system prevents an invoice number to be entered twice etc.

2. **Embedded Calculations** – These are controls that also come along with the implemented ERP. These can also be called Processing controls. These are combined with Configurable controls For example:

   (i) Depreciation calculation – The depreciation is calculated automatically by the system. This process of calculation is embedded within the ERP. However, the percentage of depreciation has to be defined for each class of asset. This is a configurable control.

   Sample depreciation configuration in Asset master:



Unit AMB Asset ID 00000000504 Executive Chairs

Trans Date 04/03/2014

Depreciation Attributes

*Book Name CORPORATE

Status Depreciable

Base Currency INR

In Service Date 07/31/2013

Begin Depr Date 07/31/2013

Convention Actual Day

Retire Conv Actual Day

*Method Straight Line

Percent

Limit Pct

Useful Life

Schedule

UOP ID

End Date

□ Special Depreciation

Depr Limit

Salvage % 5.000000000000

Multi Shift Code

Fig 3.2.2: Sample depreciation configuration in Asset master

(ii) Discount calculation - Where discounts are provided to customers based on sales value/volume

(a) Discount calculation is an embedded calculation

(b) Discount percentage is a configurable control

3. **Configurable controls** – These controls are implemented by the Company at the time of installing the ERP. These can also be called Processing controls. These will be implemented as per the process followed by the company.

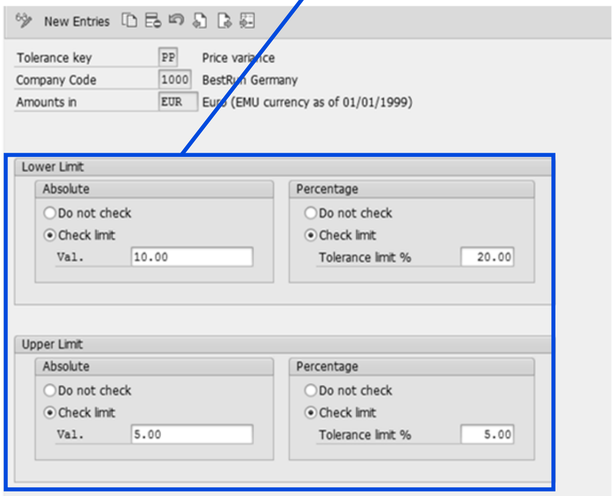
For example:

(i) 3 way match – The relevant fields within the Purchase Order (PO), Goods Received Note (GRN) and Invoice should match.

3 way match configuration in ERP

Configuration of Tolerances for price and quantity variances.

Price Variance between Purchase order and Invoice



Tolerance key	PP	Price variance
Company Code	1000	BestRun Germany
Amounts in	EUR	Euro (EMU currency as of 01/01/1999)

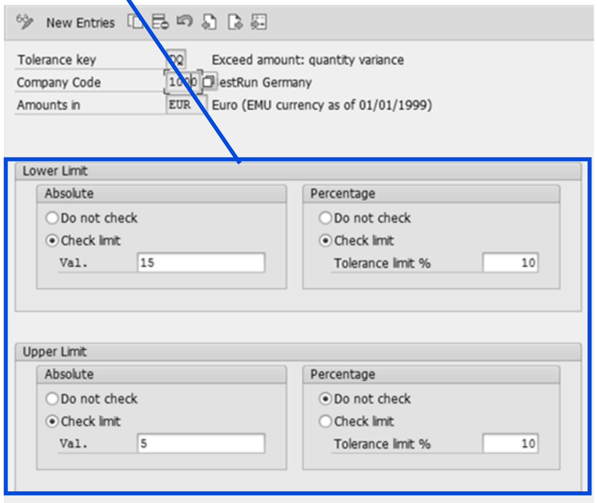
Lower Limit

Absolute	Percentage
○ Do not check	○ Do not check
● Check limit	● Check limit
Val. 10.00	Tolerance limit % 20.00

Upper Limit

Absolute	Percentage
○ Do not check	○ Do not check
● Check limit	● Check limit
Val. 5.00	Tolerance limit % 5.00

Quantity Variance between Goods Receipt and Invoice



Tolerance key	DQ	Exceed amount: quantity variance
Company Code	1000	BestRun Germany
Amounts in	EUR	Euro (EMU currency as of 01/01/1999)

Lower Limit

Absolute	Percentage
○ Do not check	○ Do not check
● Check limit	● Check limit
Val. 15	Tolerance limit % 10

Upper Limit

Absolute	Percentage
○ Do not check	● Do not check
● Check limit	○ Check limit
Val. 5	Tolerance limit % 10

Fig 3.2.3 Configuration of Tolerances

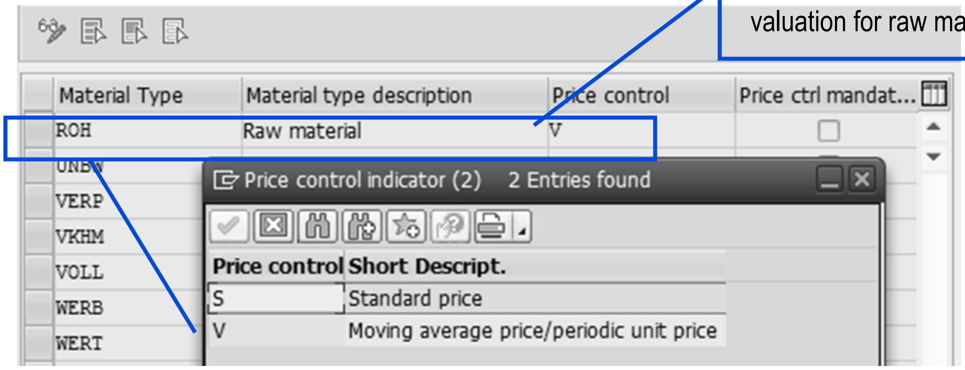
(ii) The PO raised by a Purchase Executive is approved by the Purchase Manager

(iii) At the time of raising a Sales invoice, relevant Debtors and Debtors Control account is debited and Sales account is credited.

(iv) Inventory valuation as defined by the Company – FIFO or Weighted Average etc.

Sample configuration for raw material valuation:

Configuration of Inventory valuation for raw materials



Material Type	Material type description	Price control	Price ctrl mandat...
ROH	Raw material	V	□
UNBW			
VERP			
VKHM			
VOLL			
WERB			
WERT			

Price control indicator (2) 2 Entries found

Price control	Short Descript.
S	Standard price
V	Moving average price/periodic unit price

Fig 3.2.4: Configuration of Inventory

(v) Tolerance percentage as applied by the Company in terms of discount given at the time of raising sales invoice etc.

(vi) Journals are approved based on limits set per person

4. **Access / Security controls** – Users are provided access to the systems based on their roles and responsibilities and job profiles. These can be called as Sensitive Access and Segregation of Duties. For example

(i) Data entry operator, Purchase Executive, Finance Manager, Sales Manager, CFO etc.

5. **Automated Account Posting –** Accounting entries are automatically posted in the ERP based on the business operation performed. For example

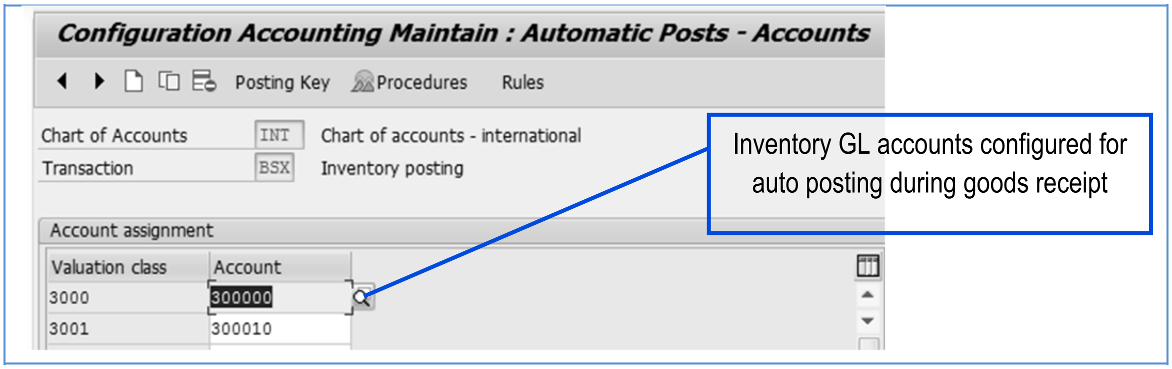
(i) Goods receipt /Issue in an ERP.

1. The operation of goods receipt triggers an automatic entry in the system:

ACCOUNT CODE	PARTCULARS	DEBIT	CREDIT
300000	Stock Account	XXXXX	
191100	To Goods Receipt account		XXXXX
301100	To Freight Clearing account		XXXXX

ACCOUNT CODE	PARTCULARS	DEBIT	CREDIT
301100	Goods Receipt account	XXXXX	
V11001	To Vendor account		XXXXX

Configuration of inventory accounts to be posted automatically during goods receipt posting:



Configuration Accounting Maintain : Automatic Posts - Accounts

Chart of Accounts INT Chart of accounts - international

Transaction BSX Inventory posting

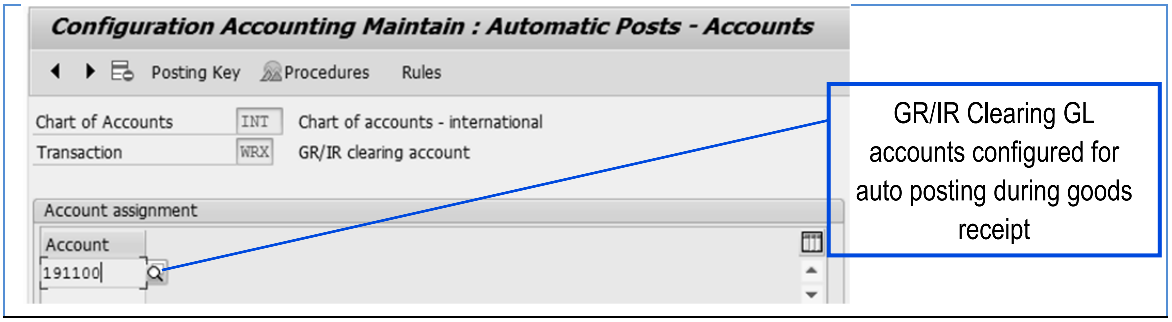
Account assignment

Valuation class	Account
3000	300000
3001	300010

Inventory GL accounts configured for auto posting during goods receipt

Fig 3.2.5: Configuration of Inventory GL accounts

Configuration of GR/IR Clearing account to be posted automatically during goods receipt posting:



Configuration Accounting Maintain : Automatic Posts - Accounts

Chart of Accounts INT Chart of accounts - international

Transaction WRX GR/IR clearing account

Account assignment

Account
191100

GR/IR Clearing GL accounts configured for auto posting during goods receipt

Fig 3.2.6: Configuration of GR/ IR Clearing GL accounts

3.3 Process of identification of Automated Application Controls

To the extent that it is relevant to an audit of financial statements, auditors are required to understand, assess and respond to such risks that arise from the use of IT systems [Ref. SA 315 (Revised) – *Identifying and assessing the risks of material misstatement through understanding the entity and its environment*].

Understanding the entity and its automated environment involves understanding how IT department is organised, IT activities, the IT dependencies, relevant risks and implemented controls.

The understanding of a company's IT environment that is obtained should be documented [Ref. SA 230 – *Audit Documentation*] using any standard format or template. This is very important to be performed in the **first year** of the audit of the company. Once this understanding is obtained and documented, the auditor should update the relevant information in the subsequent years of audit. Any changes will have an impact on the audit strategy to be adopted. This will also impact the locations from which the audit has to be conducted.

In the Introduction Chapter, we have seen a table that captures all the IT systems used by the company. Combining that table with the flow as given in the below diagram should help any an auditor to plan his audit procedures in an ERP environment.

- The auditor needs to map how each of the IT systems captured in the table contribute to the significant accounts and disclosures.
- The relevant business processes should be mapped to the IT systems.

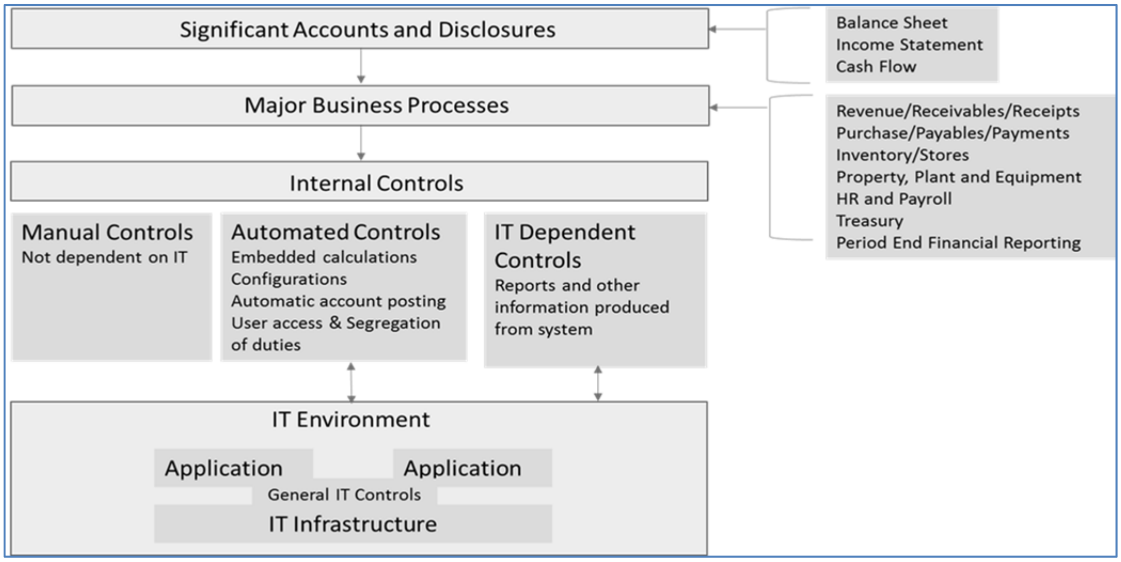


Fig 3.3.1: Process of identification of Automated Application Controls

For example:

IT system	Significant Accounts and Disclosures	Major Business Processes / Cycles	Relevant for financial reporting Y/N	Automated Controls configured within the system/Application Y/N
SAP	Sales, Debtors, Purchases, Creditors, Closing Stock etc.	Sales/ Debtors - Revenue and Receivables Purchases/Creditors – Purchase Payables Process Stock – Inventory Process	Y	Y
Pay Master	Salaries, Loans and Advances to Employees, Leave balances	HR and Payroll process	Y	Y
Interface between Paymaster and SAP	Salaries, Loans and Advances to Employees, Leave balances	HR and Payroll process and Period End Closing process	Y	Y

Once the auditor maps the relevant IT systems to Business processes and to the significant accounts and disclosures, the next step is to gain an understanding of how the business processes function and the controls within these processes. The controls can be manual, automated, IT dependent manual controls. For the purpose of this session, we shall focus only on **AACs.**

The auditor via an enquiry process gets an understanding of the various business processes. The understanding of the process flows and the controls within the processes can be documented in either of the 2 ways:

1. Process Flow Diagrams
2. Process Narratives

Process Flow Diagrams:

The Guidance Note on Internal Financial Controls over Financial Reporting refers to **Process flow diagrams** as a helpful form of documentation for auditors to depict the process to initiate, authorise, process, record and report transactions.

- Insertion of risks of material misstatement.
  - The auditor may insert symbols for risk of material misstatement at the point(s) in the process flow where the risk is present. It is possible that, due to the nature of the risk of material misstatement, it may appear at multiple points in the process flow diagram.
  - The auditor may use different symbols for significant and normal risk of material misstatement as necessary.
- Attaching control activity symbols
  - Symbols may be placed for control activity that address risks of material misstatement on the diagram.
  - Automated and manual control symbols may be used as necessary
- Identification of applications in the process flow diagram
  - If a task relies on an application system when performing an action, the auditor may use a symbol for such applications on the diagram
  - If formatting and space allows, the auditor may attach the application symbol directly on the task which it relates
- Associating the IPE symbol where appropriate
  - If IPE is used in the execution of a control activity or IPE that is produced as part of the process that is important to the audit (e.g., IPE that an auditor uses in his or her substantive procedures), the auditor may attach a separate symbol for the IPE as a document symbol.

An example of a Depreciation Run Process Flow diagram is available in Fig 3.3.2:

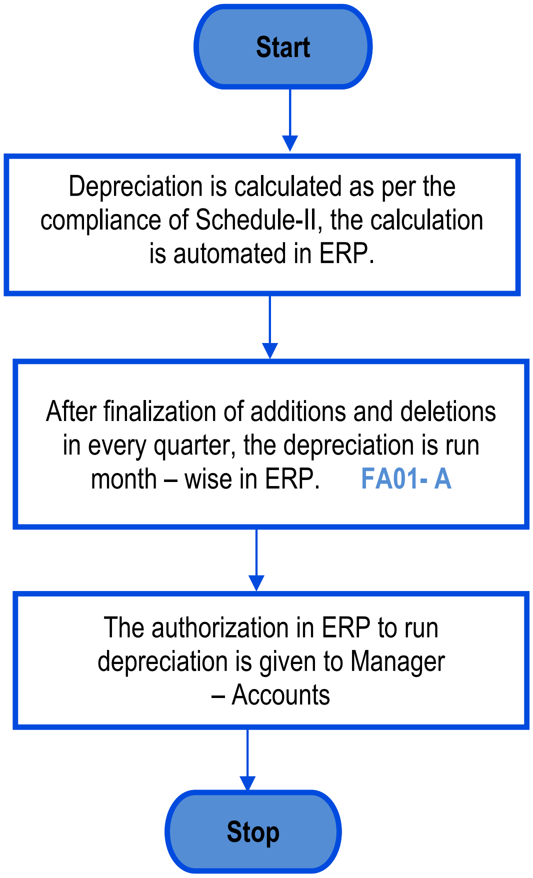

Start
Depreciation is calculated as per the compliance of Schedule-II, the calculation is automated in ERP.
After finalization of additions and deletions in every quarter, the depreciation is run month – wise in ERP.
FA01- A
The authorization in ERP to run depreciation is given to Manager – Accounts
Stop

Fig 3.3.2: Depreciation Run Process Flow diagram

FA 01 A - Automated control to run depreciation procedure.

Process Narrative:

Another form of documentation as mentioned in the Guidance Note can also be a Process Narrative to capture the process Understanding and controls within the respective Business Process. While documenting the Narrative the following points may be kept in mind:

- Who is involved in the process (e.g., departments, roles, and people)?
- Are there segregations of duties that are relevant to the process?
- What is the general objective of the processes and what are the related sub processes?
- When does the process occur?
- Does the process involve, or impact, multiple locations?-
- What are the tasks within the process and in what sequence do they occur?
- What are the points in the process at which a misstatement, including a misstatement due to fraud could arise?

- What control activities address the risks?
- What IPE is involved?
- How are application systems involved within the process?

For example: **Process Narrative for Depreciation Run Procedure:**

- The Finance Team is in charge of the depreciation run in the ERP. This is run centrally for all locations.
- Depreciation is calculated as per Schedule-II and the depreciation calculation is automated in the ERP.
- The finalization of additions and deletions are done every quarter.
- The depreciation is run month wise in the ERP via path: Transactions - Assets – Depreciation Run.
- Depreciation in the ERP can be run only on a monthly basis. The authorization in the ERP to run depreciation is given to Manager–Accounts.

Control FA 01- A = Automated

Manager-Accounts runs the depreciation after all the additions and deletions are updated by accounts team. Depreciation is automatically computed by ERP based on the asset lives entered in Asset Master.

Accounting Entries

ACCOUNT CODE	PARTCULARS	DEBIT	CREDIT
XXXXX	Depreciation on Asset Account	XXXXX	
XXXXX	To Accumulated Depreciation Account		XXXXX

Risk and Control Matrix

Process	Sub Process	Control Ref No.	Risk Description	Control Description	FSA	Frequency of Control	Manual/ Automated	Preventive/ Detective	System, IPE
Fixed Assets	Depreciation	FA-01	Depreciation calculation may be incorrect	Manager-Accounts runs the depreciation after all the additions and deletions are updated by accounts team. Depreciation is automatically computed by ERP based on the asset lives entered in Asset Master.	Accuracy	Monthly	Automated	Preventive	ERP

3.4 Procedures to review Design Effectiveness and Operating Effectiveness of Controls

The Process Narratives and Process Flow Diagrams are useful tools to document the processes followed by the Company and identify the AACs. Once the AACs are identified they have to be evaluated for Design Effectiveness. If the Design of the control is found to be effective, they have to be then tested for Operating Effectiveness.

Evaluation of Design of an AAC:

One commonly preferred method for testing Design effectiveness is a Walkthrough of the control. In a walkthrough, the auditor will track a transaction from start to end i.e. from the initiation of the transaction to the point where it is finally reported in the Financial Statements. This is very important in the first year of audits. In the subsequent years, we may update our understanding for the year based on previous years' work.

For example: For Fixed Assets cycle the process of walkthrough may be as given below as shown in Fig 3.4.1. At certain stages of the cycle, there are entries that impact the financial statements.

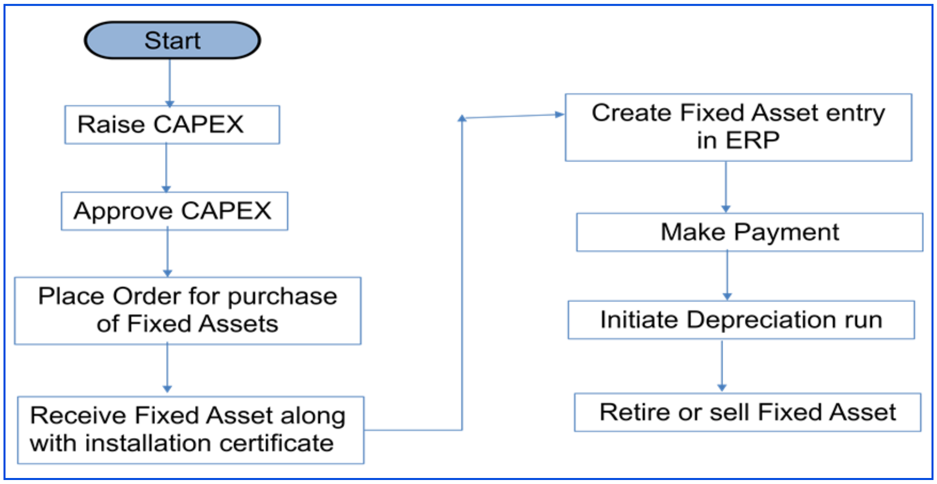

Start
Raise CAPEX
Approve CAPEX
Place Order for purchase of Fixed Assets
Receive Fixed Asset along with installation certificate
Create Fixed Asset entry in ERP
Make Payment
Initiate Depreciation run
Retire or sell Fixed Asset

Fig 3.4.1: Fixed Assets cycle the process

Management of the company is responsible for the design of the internal control. The auditor will have to evaluate this design and assess whether the control along with other controls put in place perform the function of preventing or detecting and correcting material misstatements in a timely manner. It the control is not properly designed, the risk is that it may not be able to prevent or detect errors or frauds.

Controls need to be evaluated at entity level too. Entity Level Controls are implemented to monitor the controls at the department level etc. These controls need to be designed properly by the Company and evaluated by the auditor.

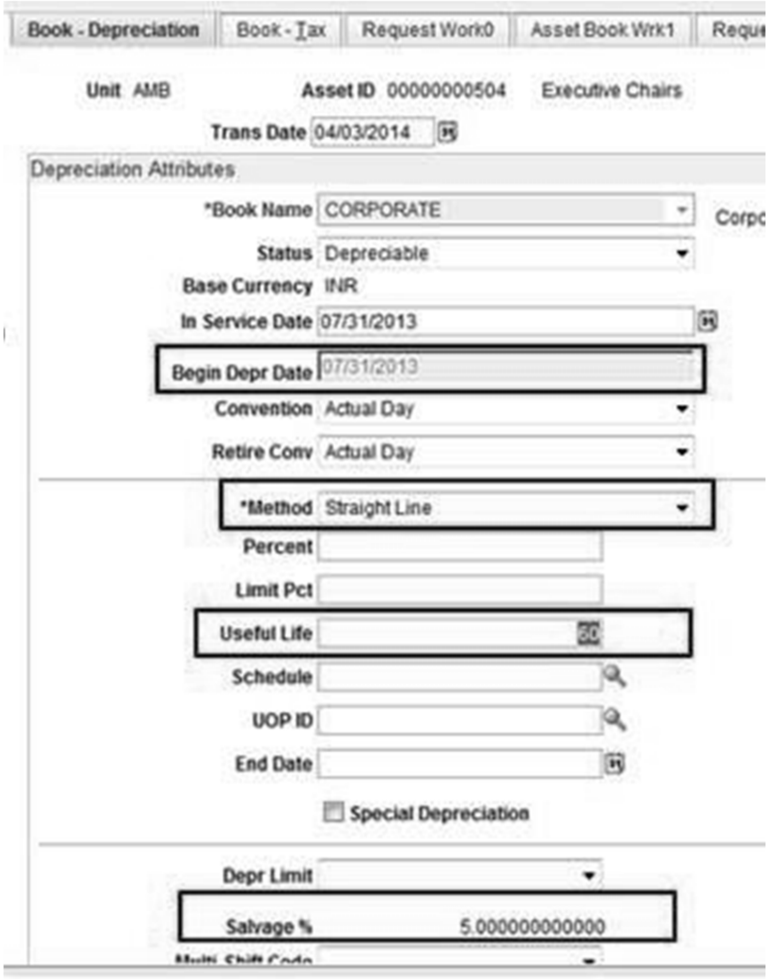
Walkthrough Procedure:

The auditor will have to adopt a combination of Inquiry, Observation and Inspection while evaluating the design of a control via Walkthrough process

- o Inquiry should be made of relevant or appropriate personnel performing the control. Probing and open ended questions to be asked of the personnel.
- o Observation of the relevant procedures performed by the personnel
- o Inspection of relevant supporting documents etc. for the control to be performed.
- o Re-performance if necessary

While testing the design of the AAC, the auditor should understand whether the logic of the control has been clearly defined in the system. The auditor will have to check the configuration in the system and understand whether it satisfies the control objective.

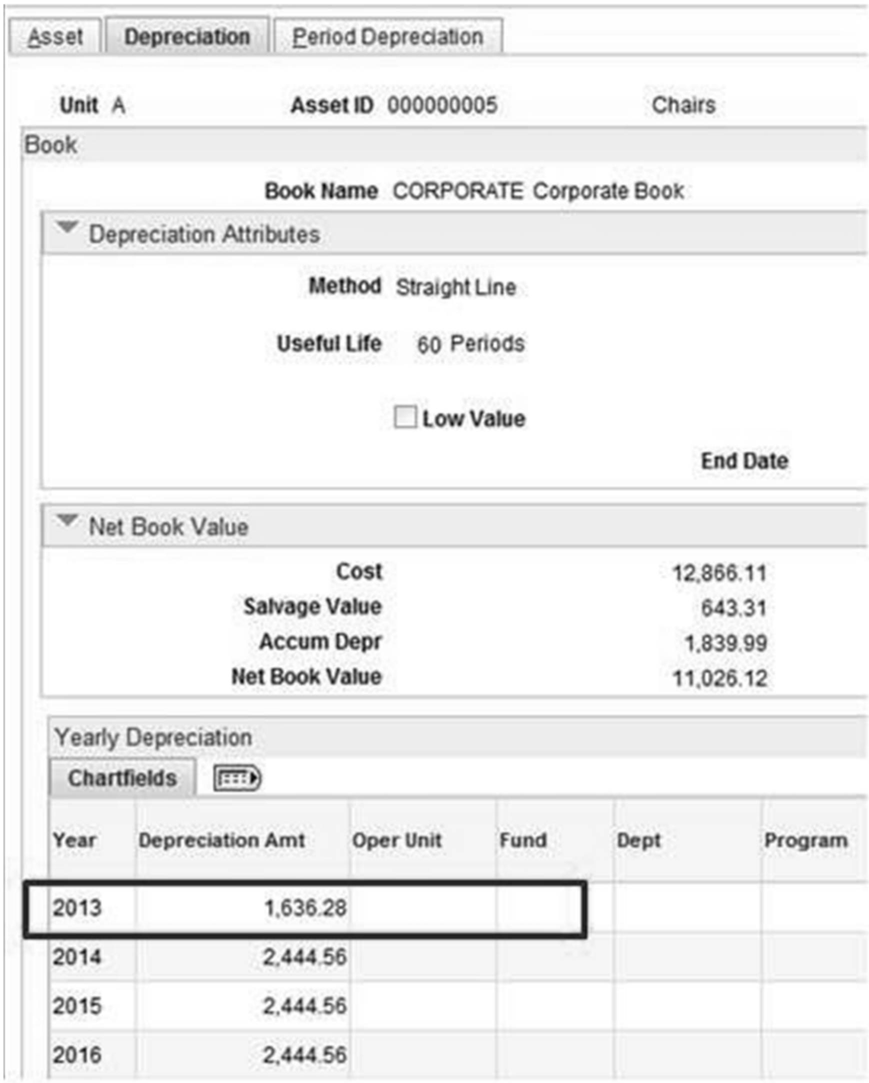
Screenshot of DEPRECIATION CALC. CONFIG



Unit	AMB
Asset ID	00000000504 Executive Chairs
Trans Date	04/03/2014
*Book Name	CORPORATE
Status	Depreciable
Base Currency	INR
In Service Date	07/31/2013
Begin Depr Date	07/31/2013
Convention	Actual Day
Retire Conv	Actual Day
*Method	Straight Line
Percent	
Limit Pct	
Useful Life	60
Schedule	
UOP ID	
End Date	
□ Special Depreciation	
Depr Limit	
Salvage %	5.000000000000
Multi Shift Code	

Fig 3.4.2: DEPRECIATION CALC. CONFIG

Walkthrough of the Depreciation control:



Unit A Asset ID 000000005 Chairs

Book

Book Name CORPORATE Corporate Book

Depreciation Attributes

Method Straight Line

Useful Life 60 Periods

□ Low Value

End Date

Net Book Value

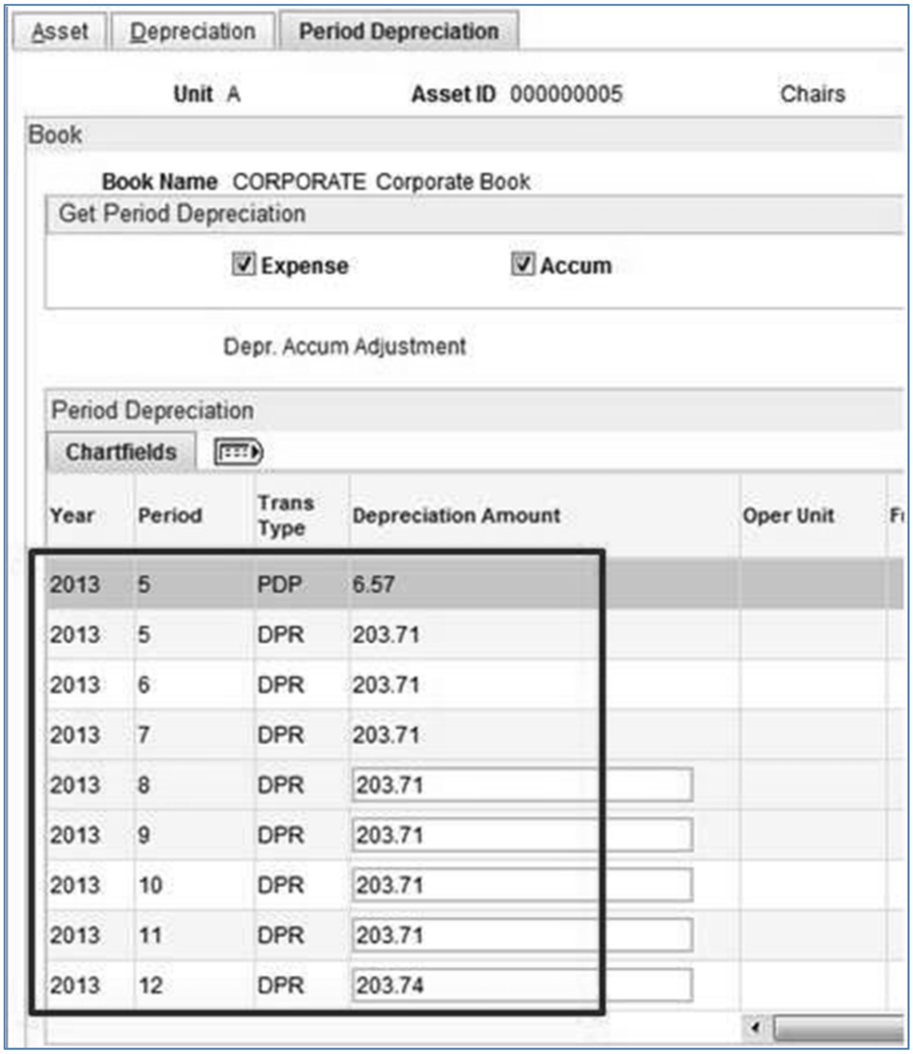
Cost	12,866.11
Salvage Value	643.31
Accum Depr	1,839.99
Net Book Value	11,026.12

Yearly Depreciation

Year	Depreciation Amt	Oper Unit	Fund	Dept	Program
2013	1,636.28				
2014	2,444.56				
2015	2,444.56				
2016	2,444.56				

Fig 3.4.3 Yearly Depreciation

DEPN1



Unit A **Asset ID** 000000005 Chairs

Book

Book Name CORPORATE Corporate Book

Get Period Depreciation

☑ **Expense** ☑ **Accum**

Depr. Accum Adjustment

Period Depreciation

Year	Period	Trans Type	Depreciation Amount	Oper Unit	Fi
2013	5	PDP	6.57		
2013	5	DPR	203.71		
2013	6	DPR	203.71		
2013	7	DPR	203.71		
2013	8	DPR	203.71		
2013	9	DPR	203.71		
2013	10	DPR	203.71		
2013	11	DPR	203.71		
2013	12	DPR	203.74		

Fig 3.4.4 Period Depreciation

DEPN 2

Control	Walkthrough Procedure	Results	Exceptions Y/N
The system automatically calculates the depreciation as per the rates defined in the system.	1. From the Asset Register select one asset that was created during the year. 2. Note the Depreciation percentage as given for the asset from the Asset register. 3. For that asset reperform the calculation of depreciation. 4. Reconcile the depreciation amount with the amount automatically calculated by the system.	Obtained the Fixed Assets Register and picked up one asset no. 000000005 – Chairs. Noted that the purchase date of the asset was 31st July 2013. Noted from the configuration that the Cost = 12866.11 Less: Salvage = 643.31 Cost = 12222.80 Useful life = 60 months Depreciation = 12222.80/60= 203.71. **Please refer to screenshot DEPN 2** Depreciation for 1 day = 203.71/31 = 6.57. **Please refer to screenshot DEPN 2** Thus total depreciation for 2013-14 = 203.71*8 = 1629.68 Depn for 31st July = 6.58 Total Depreciation 2013 =1636.26 **Please refer screenshot DEPN2**	No exceptions

The accounting entry is

Account code	Particulars	Debit	Credit
XXXXX	Depreciation on Asset Account	1636.26	
XXXXX	To Accumulated Depreciation Account		1636.26

There may be cases such as in other business cycles like Revenue cycle etc., where, there may be multiple scenarios within the cycle such as

- Multiple revenue streams
- Multiple modes of sales etc.

Note: For example If the Revenue process is different for

- Export and Domestic sales
- Cash and Credit sales

Separate transactions are to be taken for a walkthrough of each scenario. This applies for all in scope business processes.

Evaluation of Operating Effectiveness of an AAC

The auditor has evaluated the design of an AAC. Before testing the operating effectiveness of AAC, one key element to consider is the effectiveness of GITC's. As mentioned earlier, AACs are configured within the system after which the system will perform the control once it is triggered. The auditor needs to determine whether the AACs are operating as designed and whether the person operating the control has the required ability and competence to do it. The steps mentioned in the Walkthrough procedure may be used for testing the AACs.

For example: In the above example, on purchase of the Fixed Asset, at the time of creating the entry in the ERP, the company will enter details such as

- Gross Amount
- Date of Purchase / Installation
- Depreciation % or Number of months (life) for the assets to be depreciated etc.

Once these entries are configured, the depreciation is calculated automatically by the system. Hence, it is called an AAC. To add/modify/delete any of the configurations, the company will have to follow the Change Management Procedure. The authorized persons as per Company policy can only make the change in the configurations. These 2 areas fall under the Change Management and Sensitive Access and Segregation of Duties domains of GITC.

3.5 Timing of AACs testing and Sample Size

The auditor needs to plan for an appropriate time to test AACs. The factors to be considered to determine the timing to test AACs are:

- The period covered under audit

- Risk associated with the control at the time of risk assessment.

Based on the above factors the auditor will test the AACs. The assumptions before testing the AACs are:

- GITCs are effective. This is because they assist in effective functioning of application controls including AACs
- Design of the control has been evaluated and is effective.

If the GITCs are effective, then the auditor may adopt a reduced level of testing or minimal sample size. Generally, if the there are no iterations in the process and AACs then the auditor may adopt a test of one sample for testing AACs. The effectiveness of GITCs indicate that the controls operate in a similar manner throughout the period of reliance for all transactions. If there are different iterations or scenarios then the auditor will need to test each iteration/scenario while relying on the GITCs.

If there has been a change in the AAC during the audit period, then the control has to be retested after the change. Thus, at the time of planning for the audit at the beginning of the year, the auditor will have to understand from the client if there may be changes to the business processes. Accordingly, the auditor needs to plan the timing of testing AACs. The auditor should plan the timing of testing of controls after being aware that the design of the control is effective and operating for a sufficient period of time. The auditor needs to test the control for operating effectiveness at an appropriate time for the auditor to conclude that they were effective throughout the year. As per the requirements of Internal Financial Controls, the controls need to be operating as on the Balance Sheet date.

If the GITC's are found to be ineffective, then the auditor will have to test the automated controls closer to the Balance Sheet date to support the opinion on Internal Financial controls.

3.6 Assess the Impact of Deficiencies

The auditor should evaluate the identified deficiencies in controls to develop a response to risk of material misstatement as given in SA 240 "The Auditor's Responsibilities Relating to Fraud in An Audit of Financial Statements".

1. A deficiency in a Control will not allow the management to perform their assigned functions. This deficiency may not prevent or detect misstatements. Such deficiencies are called Design Deficiencies.

   A Design deficiency is also when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met.

   For example

   For a Fixed asset:

   - The Depreciation rate has not been configured OR
   - The Class of the asset has been wrongly configured

2. A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.

For example

In Payroll cycle,

- o the system is configured to calculate the Leave encashment balance. But the system is not calculating the leave balance correctly as they may be a problem in the logic within the system.

While evaluating the deficiencies, the auditor will have to check if there are any compensating controls either manual or automated and test them accordingly to check if the impact of the deficiencies is minimised.

If there are no compensating controls, the auditor may perform other procedures such as Data Analytics using CAATS tools to assess the impact of the deficiencies.

For example

- The Company has implemented an automatic approval of all Purchase Orders. The Company has a PO approval matrix and this hierarchy has been configured in the system. However, the auditor may have found out that the company has bypassed this control and placed orders based on blanket approval of Purchase orders or no approval. Thus the auditor should
    - o Obtain the complete list of all Purchase orders from the system
    - o Using CAATS identify all PO's approved as per the Approval Matrix document
    - o From the list extracted by the CAATS tool, identify all the PO's that have blank in the "Approved by field" or persons others than the Approval matrix
    - o The auditor will have to seek an explanation from the client for the reasons why the approval matrix was bypassed
    - o The auditor will have to perform other substantive procedures to obtain comfort on the Purchase amount appearing in the financial statement.

Communication of Deficiencies

SA 265 - "Communicating Deficiencies in Internal Control to Those Charged with Governance and Management" makes it necessary for the auditor to communicate control deficiencies to the Management. Prior to issuing such report the auditor may also go through the Internal audit reports and evaluate the control deficiencies identified in the reports.

The auditor must communicate in writing in sufficient advance to provide an opportunity to the company to remediate the deficiencies before the auditor issues the report on Internal Financial controls. The auditor will have to also mention if the deficiencies were present in the prior periods of audit.

NOTE: Refer Guidance on Internal Financial Controls over Financial Reporting

The auditor has identified a design deficiency in a control. Prior to the Balance sheet date, the company has rectified the design of the control. The auditor may test the implemented change for design and operating effectiveness.

3.7 Exercises

Multiple Choice Questions

1. Some of the objectives to be achieved by implementing AACs are:

   (a) Completeness

   (b) Accuracy

   (c) Both a & b

   (d) None of the above.

2. Some of the risks that are addressed by such AAC’s are:

   (a) Risk of unauthorised personnel entering the data

   (b) Risk of personnel entering unauthorised data

   (c) Risk of inaccurate processing of data

   (d) All of the above

3. Some of the examples of AACs are:

   (a) Inherent controls

   (b) Configurable controls

   (c) A and B

   (d) None of the above

4. Understanding the business process can be documented via

   (a) Flow chart

   (b) Process Narrative

   (c) Risk and Control Matrix

   (d) A and B

5. A control necessary to meet the control objective is missing. This is an example of

   (a) Significant deficiency

   (b) Operating deficiency

   (c) Design deficiency

   (d) None of the above

6. Who is responsible for the design of internal control

   (a) Internal auditor

   (b) Management

   (c) Auditor

   (d) None of the above

Fill in the Blanks

7. Validation checks and Duplicate checks performed by an ERP are part of ________________ Controls

8. Interest Computation performed by an ERP is a component of ________________ which form part of AACs.

9. The Guidance Note on Internal Financial Controls over Financial Reporting refers to ________ as a helpful form of documentation for auditors to depict the process to initiate, authorise, process, record and report transactions.

10. ______________________ is responsible for the design of the internal control.

11. The auditor will have to adopt a combination of _______, _______ and ______ while evaluating the design of a control via Walkthrough process.

12. The 3 way match of fields of PO, GRN and Invoice is an example of a _________ control.

True or False

13. If the design of an AAC is effective and prior to testing the control for operating effectiveness, it is necessary to test GITC

    (a) True

    (b) False

14. A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.

    (a) True

    (b) False

15. If there are multiple scenarios in a business cycle, it is not necessary to take one sample of each scenario to perform a walkthrough

    (a) True

    (b) False

Case Study

Access Ltd uses an ERP to capture the various operations of its business. The ERP has a fixed assets module which manages the details of the fixed assets of the company. The company informs that the fixed assets purchase procedure is automated within the system. The Purchase executive creates the asset. Based on the Asset class, the depreciation percentage is automatically populated within the system. Once created, the entry is automatically forwarded to the Fixed Asset Manager who approves the entry. For the below transaction,

- document the walkthrough of the automated controls,
- evaluate the design of the automated controls
- test the operating effectiveness of the controls

Assumption: GITCs are effective.

Other details:

Invoice No. Access/1718/22 dated 1st April 2017.
Asset No.: PM01-1718
Asset purchased: Plant & machinery
Asset class: Plant & machinery
Amount: Rs 1000000 (Ten lakhs)
Date of Purchase: 1st April 2017

3.8 References and Other Reading Material

1. Standards on Auditing published by the Institute of Chartered Accountants of India (ICAI), www.icai.org > Resources

2. Guidance Note on Audit of Internal Financial Controls Over Financial Reporting issued by Auditing and Assurance Standards Board. - (14-09-2015), www.icai.org

3. Companies Act 2013, www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf

3.9 Answers to Exercise

1 Correct answer is (c) – Completeness and Accuracy are the two objectives of implementing AACs. Other objectives are validity, segregation of duties etc.

2 Correct answer is (d) – All of the above

All the mentioned risks are addressed by AACs

3 Correct answer is (c)

Inherent, configurable, automated calculations etc. are AACs.

4 Correct answer is (d)

Flow chart and Process Narratives are 2 ways of documenting business processes

5 Correct answer is (c).

If a control is missing it is an example of Design deficiency.

6 Correct answer is (b)

Management is responsible for design of controls. Internal auditors and Auditor are responsible for testing the controls.

Fill in the Blanks

7 Inherent

8 Automated calculations.

9 Process flow diagrams.

10 Management.

11 Inquiry, Observation and Inspection.

12 Configurable.

True or False

13 True. GITCs have to be effective, to have a strategy to test AACs for operating effectiveness.

14 True. Operating effectiveness deficiency exists when the control does not operate as expected or the person operating the control is not competent.

15 False. If there are different scenarios in a business process, then one transaction per scenario have to be taken for a walkthrough.

Answer to Case Study

Access Ltd.

Process : Fixed Asset

Sub - Process : Fixed Asset

Activity: Creation of Asset Master

Walkthrough Documentation

Date Performed : xx/xx/xx17

Performed By : AAAA

Client representative : BBBB

Ref	Process or Control	Activity/ Control	Walk- through Plan	Walk-through Procedure performed	Systems reports or spreadsheets relied on	Evidence Examined	Design Effectiveness	Operating Effectiveness	Gaps if any	Report to Client
a)	From the ERP, obtain a list of all Fixed asset purchases made during the year 2017-18.	Activity	Check whether parameters are given correctly in the ERP to extract the listing	Obtained the Fixed asset additions report for the year 2017-18 and tallied it with the amount appearing in Trial Balance.	Fixed Assets Purchases Listing	Fixed Assets Purchases Listing		None	None	Not Applicable
b)	From the Fixed Asset Register obtain details of the Asset No to be taken for walkthrough.	Activity	From the Fixed Assets register, obtain the Fixed assets details. Obtain the invoice number entered there and check if the same is given in Purchase Listing	Obtained Asset No. PM01-1718 and corresponding Invoice no. Checked whether the Invoice number is available in the Purchase Listing	Fixed Assets Purchases Listing Fixed Assets Register	1. Fixed Assets Purchases Listing 2. Fixed Assets Register 3. Invoice No. Access/1718/22 dated 1st April 2017	None	None	None	Not Applicable

c)	Match invoice details with Fixed Assets Register	Activity	Obtain hard copy of original invoice number and match the details of class of Fixed Assets Purchased with Fixed Assets Register	From Invoice Number Access/1718/22 dated 1st April 2017 understood that asset purchased was Plant and Machinery. With the help of the Purchase Executive, checked the details in the ERP with regard to the Asset. Noted that the categorisation was correct. Invoice date is 1st April 2017.	None	1. The details in the ERP 2. Invoice No. Access/1718/22	None	None	None	Not Applicable
d)	Depreciation rate is populated automatically by the ERP	Control	Check in the system, the process of population of depreciation rates for the Fixed Assets category.	Noted that based on the categorisation, the depreciation rate is automatically populated. Noted in the ERP that depreciation rate is given correctly as 6.33%	ERP	ERP	Yes	Yes	None	None
e)	The fixed asset entry is automatically approved by the Fixed Asset Manager	Control	Check in the system, the process of automatic approval by Fixed Assets Manager	For the approval of the asset, noticed the drop down list in the ERP. The list had only one name i.e., of Fixed Asset Manager, who approved the entry	ERP	ERP	Yes	Yes	None	None

3.10 Glossary

AAC – Automated Application Controls

SEC – Securities and Exchange Commission

SOX – Sarbanes Oxley Act 2002

ICFR – Internal Controls over Financial Reporting.

COSO – Committee of the Sponsoring Organisations of the Treadway Commission

CAPEX – Capital Expense

CHAPTER 4

SEGREGATION OF DUTIES AND SENSITIVE ACCESS

LEARNING OBJECTIVES

- To understand what is meant by segregation of duties and sensitive access
- To understand about roles and profiles in an ERP environment
- To understand the methods and procedures to review segregation of duties and sensitive access
- To understand how to assess the impact of conclusions of GITCs on segregation of duties and sensitive access
- To understand how to determine and evaluate impact of deficiencies in segregation of duties and sensitive access on overall audit

4.1 What is Segregation of Duties and Sensitive Access

4.1.1 Sensitive Access (SA)

Sensitive access is when a user has the ability to perform critical business activities in an ERP. In other words, business activities that carry a higher risk and could have wider impact on operations are referred to as sensitive activities and the users who have this access are said to have sensitive access. Examples of sensitive access in an ERP can include ability to

- create and modify sales prices
- approve purchase orders
- master data
- payroll information
- foreign exchange rates
- period open/closure function

4.1.2 Segregation of Duties (SOD)

Segregation of duties refers to the separation or distribution of job roles among employees in such a way that incompatible or conflicting job roles are assigned to different persons.

- **For example:** preparation of a journal entry and approval of that journal are assigned to two different persons. This is because if the same person prepares and approves a journal entry, there is a risk of

  (a) unauthorised journal entry being posted

  (b) errors in journal entry may not be identified and corrected in a timely manner

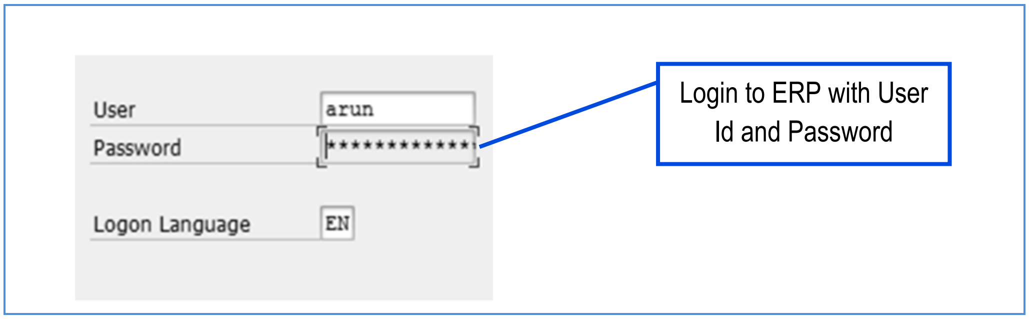
The concept of segregation of duties existed in business as part of the internal control procedures even before the IT systems and ERPs came into use.

- **For example**: in a manual system of accounting and book keeping, hard copy cash vouchers are prepared by the cashier, reviewed by the accountant and authorised by the accounts manager before the transaction is posted to ledgers.

With ERPs now being used extensively, segregation of duties is being implemented and enforced through the user access controls feature of ERP.

4.1.3 User Access in ERP

One of the key feature of an ERP is the ability to control users access to relevant business functions, activities and operations within the ERP. Every person or individual who uses an ERP is called a "user" of the ERP and each such user is assigned an identification called "user id" along with a corresponding secret code called "password". While the user id is known to all, the password is known only to the person or individual to whom the user id is assigned. The combination of user id and password makes it possible for a person to start using the ERP as shown in Fig 4.1.1.



User arun

Password ************

Logon Language EN

Login to ERP with User Id and Password

Fig 4.1.1 Login to ERP

There are several types of users within an ERP, they are

Normal users: These users are typically regular employees who carry out day-to-day business operations and transactions using the ERP. For example, the employees who process sales orders, invoices, stores receipts & issues, processing journal entries, are known as normal users, end users or business users.

System users: These users are internally used within the ERP to perform automated operations and transactions.

- **For example:** automatic posting of monthly accrual entries, batch operations, process period-end routines, interface with other systems and sub-systems are some operations performed using system users viz., WF-BATCH, SYSTEM

Privileged users: These are a type of super users who have very extensive or unlimited access to carry out all or several activities in an ERP environment.

- **For example:** administrators, functional consultants or some ERP support teams are some of the common super users viz., Admin, Administrator, BASIS, SYS

Default users: These are users that come packaged along with the ERP software. These users are sometimes required to setup the ERP system initially. They are also used for educational purposes, when updating the ERP to newer versions, to facilitate remote monitoring by vendors.

Generic users: These are similar to normal users but named in such a way that represent a title, position, designation or function, place or region within a company and do not represent an individual or person.

- **For example:** users named CMD, CEO, MD, CFO, VP, Mumbai Region, Delhi Branch are generic users. In this case even though the users are not given personal names, the user id is assigned to a single person at a given point in time.

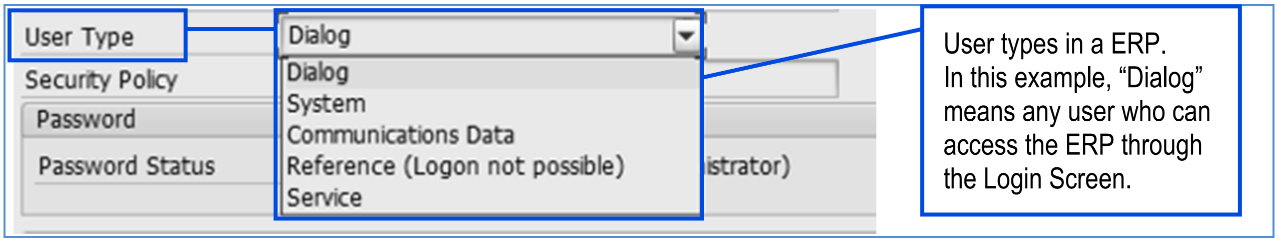
There is another type of generic users who share a common user id. For example, Sales User could be an id shared by all persons in the sales department.

Temporary users: As the name suggests, these are users who are given user id for a limited time period. For example, guest users, auditors, consultants and support users.

External users: These are users who do not belong to the company i.e., they are not employees but they may still require access to the ERP. For example, vendors, customers, business partners.

We can see that there are several types of users of an ERP that we need to understand and not all user ids are necessarily assigned to persons. While the types of users mentioned above are commonly seen in an ERP environment, it is possible that there are more user types depending on the company policies and ERP product design, specifications and the way it has been implemented in a company. The user types and the terminology used to categorise user types could vary between different ERPs.

The auditor should understand the various types of users that exist in an ERP environment before reviewing segregation of duties and sensitive access as shown in Fig 4.1.2.



User Type: Dialog

User types in a ERP.
In this example, “Dialog” means any user who can access the ERP through the Login Screen.

Fig 4.1.2 Users Type

User access to an ERP is given on a need-to-know and need-to-do basis. All users will not have access to all the functions of the ERP. In other words, users access to ERP is based on the job roles and responsibilities of respective users.

- **For example:** A Store Manager whose job to process and maintain stores inventory, receipts and issues will have access to process goods receipts, goods issues and stock movements.

4.2 Roles and Profiles

4.2.1 Using ERP Roles for implementing Segregation of Duties and Sensitive Access

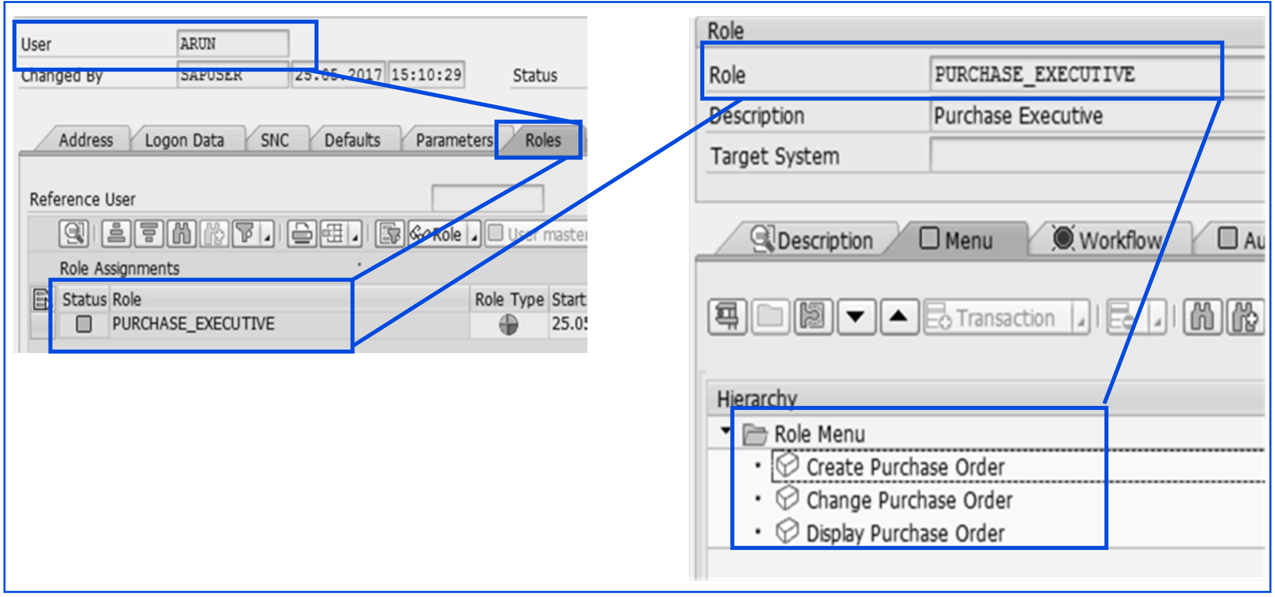
Roles and Profiles are access control features in an ERP that enable grouping of several related access rights in to a form which is logical and easy to manage and maintain.

- **For example:** users in a purchase department may typically need to perform activities including creation of purchase orders, change purchase orders and display or view purchase orders. Users in the department should be provided access to each of these activities individually in the ERP.

In a small ERP environment where there are 2-5 users, this may not be difficult but imagine in a larger ERP environment with 20-50 users providing access to each activity may be more time consuming and prone to errors. However, by grouping the purchase activities into a role it is much faster and easier to assign access to all users with reduced chance for error.

The relationship between ERP Roles and users is many-to-many. For example, One ERP role Purchase_Executive can be assigned to many users. On the other hand, one user Arun could be assigned more than one ERP roles.

In the example below, three purchase activities a) Create Purchase Order, b) Change Purchase Order and c) Display Purchase Order have been grouped together to create a role named Purchase_Executive. This role has been assigned to a user named Arun who works in the purchase department.



User ARUN
Changed By SAPUSER 25.05.2017 15:10:29 Status

Reference User

Role Assignments

Status	Role	Role Type	Start
□	PURCHASE_EXECUTIVE		25.05

Role

Role PURCHASE_EXECUTIVE
Description Purchase Executive
Target System

Hierarchy
- Role Menu
  - Create Purchase Order
  - Change Purchase Order
  - Display Purchase Order

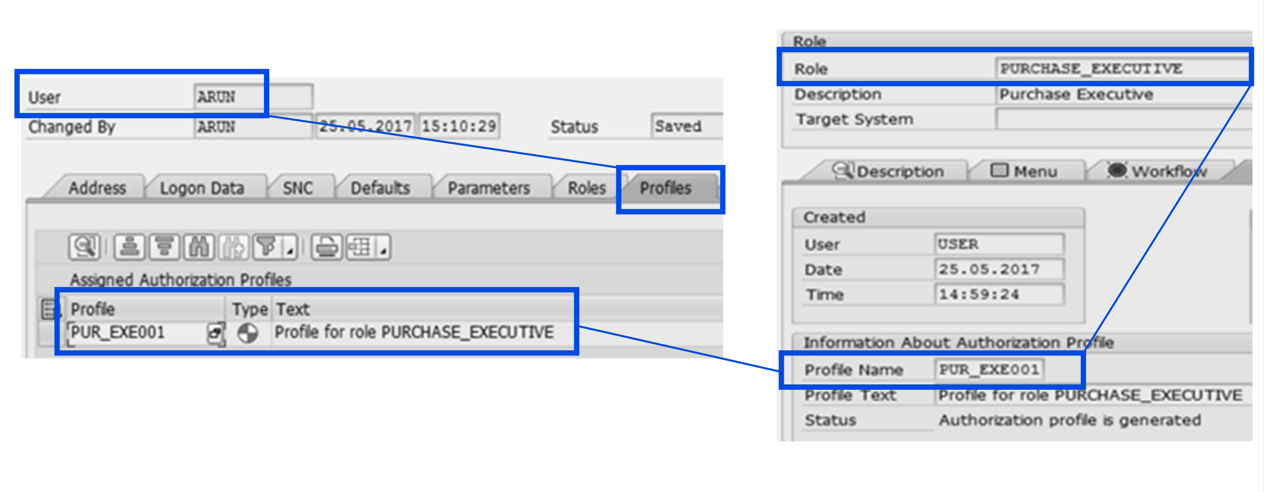
Fig 4.2.1 Roles and Profile

Roles offer an easy to understand, fast and reliable way to manage user access to an ERP. Generally, Roles are defined at the time of implementation of the ERP based on the job functions of employees. In ERP terms this feature is known as Role Based Access Control (RBAC).

4.2.2 Using ERP Profiles for implementing Segregation of Duties and Sensitive Access

A Profile is also a feature that is available in ERPs that is useful in implementing user access security and controls. The basic purpose of a profile is similar to that of a role, i.e., to group related access in a logical form. While a role represents a high-level grouping, which is aligned closely with the business function and job responsibilities of a user, a profile is the more granular internal technical grouping of authorisations, permissions and access rights within the ERP based on the input derived from the Role.

In the below example as shown in Fig 4.2.2, we can see that a profile named PUR_EXE001 has been created for the role Purchase_Executive. This profile has then been assigned to the user.



User ARUN
Changed By ARUN 25.05.2017 15:10:29 Status Saved

Assigned Authorization Profiles

Profile	Type	Text
PUR_EXE001		Profile for role PURCHASE_EXECUTIVE

Role
Role PURCHASE_EXECUTIVE
Description Purchase Executive
Target System

Created
User USER
Date 25.05.2017
Time 14:59:24

Information About Authorization Profile
Profile Name PUR_EXE001
Profile Text Profile for role PURCHASE_EXECUTIVE
Status Authorization profile is generated

Fig 4.2.2 ERP Profile

4.3 Procedures for Review

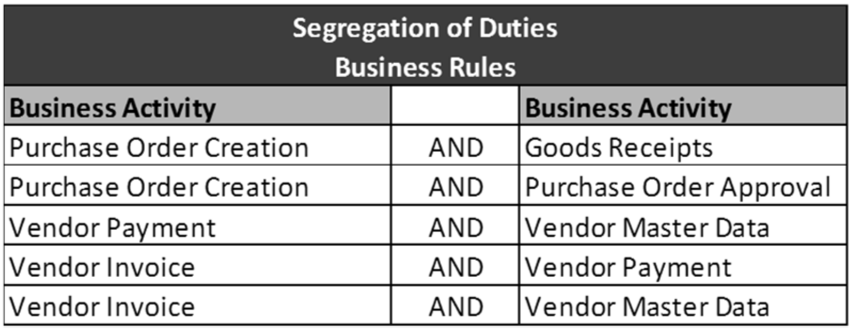
To audit segregation of duties and sensitive access in an ERP environment, the auditor first needs to understand the business and IT environment in which company operates including the following,

(a) understand the various business functions, organisation structure, employee job roles and responsibilities.

(b) the process that is followed for managing user access to ERP

(c) Understand the rules based on which user access has been implemented in the ERP

Given below as shown in Fig 4.3.1 is an example of business rules for implementing segregation of duties in a Purchase and Payables business process. The combination of two different business abilities or business activities mentioned below, when given to the same user(s), creates a conflict and could compromise the segregation of duties.



Segregation of Duties Business Rules		
Business Activity		Business Activity
Purchase Order Creation	AND	Goods Receipts
Purchase Order Creation	AND	Purchase Order Approval
Vendor Payment	AND	Vendor Master Data
Vendor Invoice	AND	Vendor Payment
Vendor Invoice	AND	Vendor Master Data

Fig 4.3.1 Segregation of Duties

Having obtained this understanding, the auditor should determine, based on the audit risk assessment, which segregation of duties rules and sensitive access are relevant to audit and accordingly prepare an audit test plan.

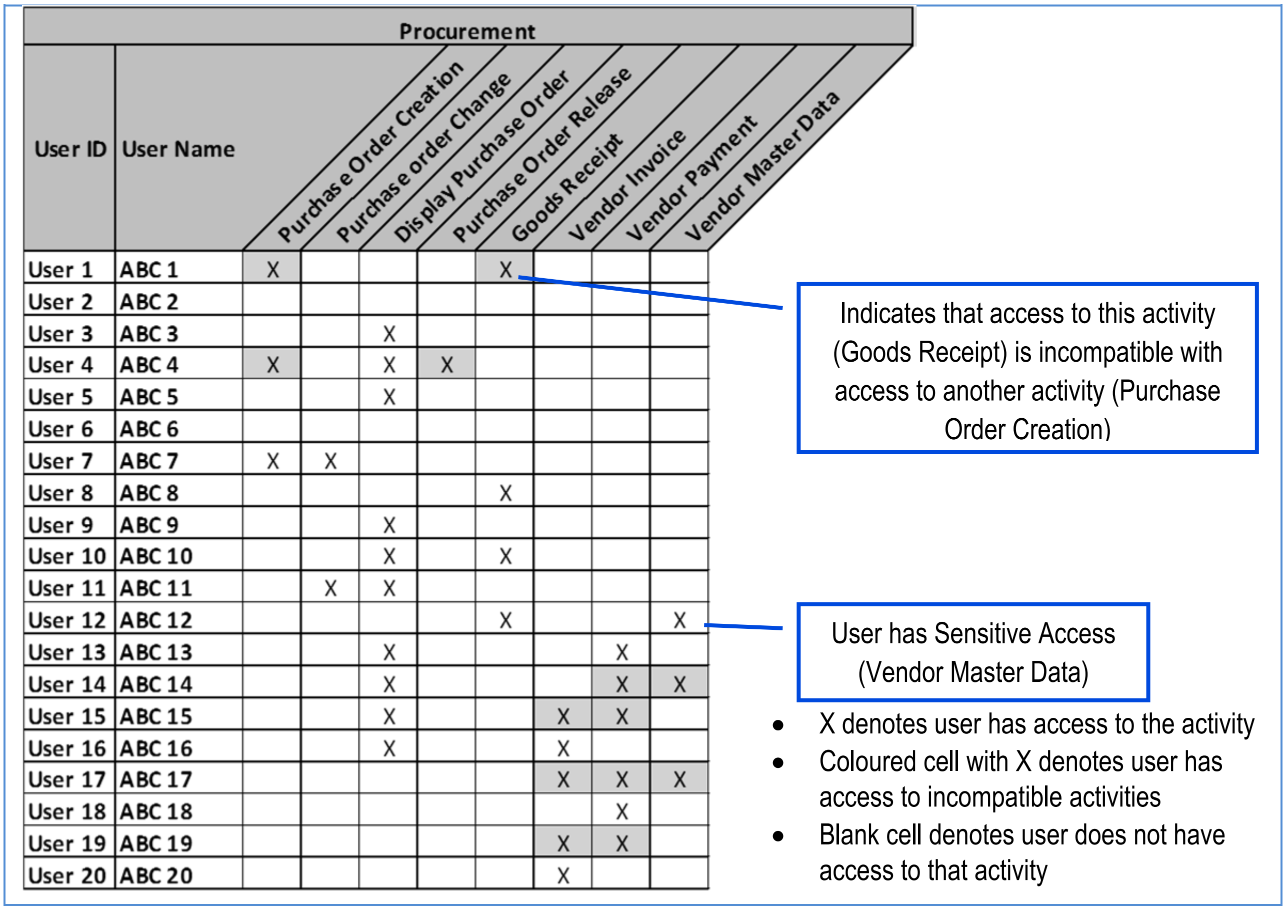
Segregation of duties can be implemented as preventive or detective control. When implemented as a preventive control, the user access requests are first checked with the company's predefined segregation of duties rules before access is provided. Any deviations between the access requested and the rules are identified and resolved and access to incompatible activities are denied upfront.

In case segregation of duties are implemented as a detective control, user access is provided first and a periodic check (say, every month or quarter) are performed to detect deviations in the user access and segregation of duties rules. Deviations are resolved by revoking the user access to incompatible activities.

Identification and review of user access controls including segregation of duties and sensitive access can be very complicated to review in an ERP environment due to the number of users, several access rules, the possible combinations and their outcomes all of which could run into several hundreds, thousands or even more for large ERP environments. Hence, it is common to use specialised automated tools for the review of segregation of duties and sensitive access. Even though this review can be performed manually, using tools makes the review process more effective and efficient. However, the auditor should receive adequate training prior to using such specialised audit tools and techniques.

- **For example:** some of the tools that are used in implementing and review of segregation of duties and sensitive access include SAP GRC (formerly, Virsa), Oracle GRC, BIZRights, Proprietary tools.

Given below is an example of how the user access in ERP can be summarised for a business activities as shown in Fig 4.3.2



		Procurement							
User ID	User Name	Purchase Order Creation	Purchase order Change	Display Purchase Order	Purchase Order Release	Goods Receipt	Vendor Invoice	Vendor Payment	Vendor Master Data
User 1	ABC 1	X				X			
User 2	ABC 2								
User 3	ABC 3			X					
User 4	ABC 4	X		X	X				
User 5	ABC 5			X					
User 6	ABC 6								
User 7	ABC 7	X	X						
User 8	ABC 8					X			
User 9	ABC 9			X					
User 10	ABC 10			X		X			
User 11	ABC 11		X	X					
User 12	ABC 12					X			X
User 13	ABC 13			X				X	
User 14	ABC 14			X				X	X
User 15	ABC 15			X			X	X	
User 16	ABC 16			X			X		
User 17	ABC 17						X	X	X
User 18	ABC 18							X	
User 19	ABC 19						X	X	
User 20	ABC 20						X		

Indicates that access to this activity (Goods Receipt) is incompatible with access to another activity (Purchase Order Creation)

User has Sensitive Access (Vendor Master Data)

- X denotes user has access to the activity
- Coloured cell with X denotes user has access to incompatible activities
- Blank cell denotes user does not have access to that activity

Fig 4.3.2 User access in ERP

4.4 Impact of conclusions of GITCs

Implementing and maintaining segregation of duties and sensitive access in an ERP environment is a very dynamic process that keeps changing all the time due to the changes in business environment. For example, employees change, job roles change, processes change and systems change. Whenever such changes in business environment occur, the corresponding changes in user access must be made in the ERP environment too. When an auditor reviews the user access controls in an ERP, the review is done at a point-in-time and the results represent users access at that point only. However, auditing standards require auditors to obtain evidence for the full period of audit.

This is where the effectiveness of GITCs becomes relevant. GITCs are General Information Technology Controls that support the operating effectiveness of automated application controls and IT dependent controls. User access controls are like application controls in an ERP environment and dependent on GITCs.

When GITCs are designed and operating effectively for the entire audit period, the auditor can conclude that user access controls, including segregation of duties and sensitive access, are operating effectively throughout the same period even though testing was performed point-in-time.

If there are deficiencies in GITCs or when they are not effective, it is likely to have an impact on the design and operating effectiveness of application controls including user access controls. The auditor may have to carry out additional testing and gather more audit evidence to conclude on the effectiveness of user access controls that include segregation of duties and sensitive access.

4.5 Conclusion on Impact of Deficiencies on audit

During a review of segregation of duties and sensitive access the auditor may find deficiencies in the user access controls. Examples of such deficiencies are given below:

(a) some users have access to prepare a purchase order and approve the same purchase order

(b) users have access to maintain vendor master data and process vendor payments

(c) users in sales department have access to maintain payroll information

(d) IT department users have access to process business transactions

Having found deficiencies, the auditor should evaluate the impact of these deficiencies on the audit. For this evaluation, the auditor should consider the following:

- Is there a business reason because of which the segregation of duties could not be implemented in the ERP?
- In case of business reason, has management identified a suitable compensating control.
- Can we test the compensating control?
- Has any user actually used the access? This means, a user has been inadvertently given access to incompatible functions in the ERP, but the user was not aware of this and never actually used this access.
- Are there any manual controls that mitigate the lack of user access controls? For example, there could be a manual control where all purchase orders are manually signed by a higher-level employee viz., a Purchase Director or Managing Director or CEO.
- For instances where a user has actually used the access, can management provide a list of all such instances and ratify them all and confirm validity of transactions. The auditor may also consider determining aggregate financial impact of the deficiency and evaluate the same from a materiality viewpoint.

The above examples are some of the ways in which the auditor thinks through the deficiencies and assess impact on audit. Wherever necessary, the auditor may have to obtain additional audit evidence to address the risk of material misstatement.

4.6 Exercises

Multiple Choice Questions

1. Which of the following is NOT an example of an External user type,

   (a) Employees

(b) Customers

(c) Vendors

(d) None of the above

2. Business rules for implementing segregation of duties are defined by

(a) ERP Consultants

(b) Government

(c) Company

(d) Statutory Auditors

3. Examples of specialised tools to review segregation of duties and sensitive access in an ERP include,

(a) SAP GRC.

(b) Proprietary tools

(c) BIZ Rights

(d) All of the above.

4. Auditors review of user access controls in an ERP environment is performed at a point-in-time. What other controls can auditors rely upon to get evidence of operating effectiveness for full year.

(a) Compensating Controls

(b) General IT Controls

(c) Manual Controls

(d) Automated Controls

5. When an auditor finds a deficiency in the user access controls, what should the auditor do next

(a) Report deficiency to management and do nothing more.

(b) Increase substantive testing

(c) Ignore the deficiency

(d) Evaluate the deficiency and determine impact on audit

Fill in the blanks

6. Sensitive access in an ERP refers to the ability of a user to perform _______ business activities.

7. Super users who have very extensive or unlimited access to carry out all or several activities in an ERP environment are also known as _______ users.

8. The auditor should first gain and understanding of the ________ and ________ environments before auditing segregation of duties and sensitive access in an ERP.

9. Segregation of duties can be implemented as either ______ or ______ controls.

10. ______ make it easy to manage user access to an ERP

True/False

11. Segregation of duties can be implemented only in companies that use ERP (True/False)

12. Business Rules for implementing segregation of duties should be defined by the auditor (True/False)

13. A user in purchase department has access to maintain vendor master data and process vendor invoices. This indicates a deficiency in segregation of duties (True/False)

14. User access to an ERP is given based on user job roles and responsibilities (True/False)

15. Reliability of user access controls in an ERP depend on effectiveness of application controls (True/False)

4.7 Case study

Access Ltd is a Private Limited Company which is in the business of manufacturing and selling mobile phones within India. Revenues in FY17 is INR 100 crores. Access Ltd is using an ERP for all business operations including Revenue and Receivables functions. You are auditing Access Ltd for FY17 and based on your understanding of business and IT environment you have determined the following:

(a) There are 10 users (User01 to User10) in the ERP who have access to do the following activities:

- All users can process Sales orders
- User03, User04 and User05 can process despatches
- User06, User07, User08 can process sales invoices
- User01 can maintain customer master and price master
- User09 belongs to Finance/Accounts and has access to process bank receipts/collections
- User10 belongs to IT has access do all activities

(b) The company has given ERP access as per business requirements but do not have documented business rules for segregation of duties.

(c) You have reviewed the General IT controls and found them to be effective

Your task is,

(a) Based on your risk assessment identify any five combinations of business activities in the Revenue and Receivables process where segregation of duties should exist.

(b) Identify the activities that are considered as sensitive access

(c) Prepare a list of your observations, if any

4.8 References and Further Reading

1. Standards on Auditing published by the Institute of Chartered Accountants of India (ICAI), www.icai.org > Resources

2. Guidance Note on Audit of Internal Financial Controls Over Financial Reporting issued by Auditing and Assurance Standards Board. - (14-09-2015), www.icai.org

3. Companies Act 2013, www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf

4.9 Answers to Excises

1. Correct answer is (A).

   Employees are typically considered as normal users or end users because they belong to a company, not external.

   (B), (C) Vendors, Customers are generally classified as external users.

2. Correct answer is (C).

   Company policy should define the rules for segregation of duties as part of the internal control framework.

   (A) ERP consultants can help in the implementation of user access controls in ERP to comply with company policy on segregation of duties.

   (B) Government does not define rules for segregation of duties for a specific company. However, local laws and regulations should be considered when defining the company policy.

   (D) Statutory auditors will review and test user access controls in ERP including segregation of duties based on the risk assessment. However, auditors cannot define the rules for segregation of duties.

3. Correct answer is (D). All the mentioned tools can be used.

4. Correct answer is (B).

   When General IT Controls (GITCs) are effective for full year, the auditor can rely on user access controls for the same period.

   (A) Compensating controls are considered when a deficiency is found.

   (C) Manual controls do not provide assurance for the operating effectiveness of user access controls.

   (D) Automated controls are business process controls that also depend on effectiveness of GITC

5. Correct answer is (D)

   The auditor should evaluate each deficiency and determine impact on audit. The auditor should consider several mitigating factors and compensating controls and obtain additional audit evidence, if necessary.

   (A) All deficiencies should be reported to management. In addition, auditor should evaluate each deficiency.

   (B) The auditor may consider more substantive testing only if necessary. But first, the auditor should evaluate the deficiency.

   (D) Deficiencies should not be ignored.

6. Critical
7. Privileged
8. Business, IT
9. Preventive, Detective
10. Roles
11. False. Segregation of duties is implemented even in companies where there is no ERP.
12. False. Business rules for implementing segregation of duties should be defined by the company/management.
13. True.
14. True.
15. False. Reliability of user access controls in ERP depend on the effectiveness of General IT Controls.

4.10 Case Study Solution

(a) There could be several conflicting combinations of business activities where segregation of duties should be applied. However, it is based on risk assessment and professional judgement. Five such SOD combinations are as follows:

Process Sale Orders	AND	Maintain Master Data
Process Sale Orders	AND	Process Invoices
Process Despatches	AND	Process Receipts/Collections
Process Invoices	AND	Process Receipts/Collections
Process Receipts/Collections	AND	Maintain Master Data

(b) Maintain Master Data and Process Receipts/Collections could be considered as Sensitive Access

(c) Some of the observations are as follows.

- Company does not have documented business rules for implementing segregation of duties.
- There are instances where segregation of duties does not exist (based on the rules mentioned in a) above
- IT users have access to all activities in the Revenue and Receivables process.
- User01 has access to maintain master data and also process sale orders
- Users06, User07, User08 can process sales orders and also invoices

Note: It is suggested that the auditor prepare a chart of all ERP users and their access to business activities in a matrix format. This will be useful in evaluating the segregation of duties and sensitive access more effectively and efficiently.

4.11 Glossary

ERP – Enterprise Resource Planning

SOD – Segregation of duties

SA – Sensitive Access

GITC – General Information Technology Controls

Role – is a logical grouping of users in an ERP that is aligned to a job function

Profile – is an internal technical grouping of authorisations, permissions and user access rights in an ERP and is derived from a role

GRC – Governance, Risk and Compliance

CHAPTER 5

SYSTEM GENERATED REPORTS

LEARNING OBJECTIVES

- To understand Types of reports - Standard Reports, Customized Reports, Database Queries
- To understand procedures for validation of Reports - accuracy of logic, completeness and accuracy of data
- To understand the impact of conclusions of GITCs on Report testing
- To understand conclusion of impact of deficiencies in Report testing on audit
- To understand when to test.

5.1 Overview

As businesses reliance on ERP systems and applications is on the increase, the information available in these systems become critical. This information or data is critical for decision making or even for compliance purposes for ROC etc. and is relied upon by the various stakeholders of an entity such as the management, auditors etc. Thus the integrity of the information / data etc. on which the stakeholders make decisions becomes crucial. As per the Guidance Note issued by the Institute on Audit of Internal Financial Controls over Financial Reporting, the data or Information Produced by the Entity (IPE) can be generally used for:

- IPE is used by entity personnel to perform a relevant control.
- IPE is used by the auditor to test a relevant control.
- IPE is used by the auditor to perform substantive procedures.

The IPE can be in 2 forms:

- Reports generated from the System
- Listing/Output created manually with data from the system.

In this session, we shall focus more on understanding the different types of reports, procedures to test them and impact of the testing performed.

Some examples of reports are high level reports such as Cash Flow statement, Analysis of Obsolete inventory or more microscopic level of reports such as Registers – Purchase, Sales or Debtors Aging analysis etc. Profit and Loss account, Balance Sheet can also be termed reports.

5.1.1 Why to test reports

- Management may make decisions relating to investments, efficiency of operations, allocation of funds to different business streams etc.
- Management may have implemented various manual controls within the business processes. These manual controls might be dependent on an underlying report from the system.

For example –

- A Periodic review of a Cash Flow statement by the Finance team.
- Provision of bad and doubtful debts. The finance team extracts a report from the system which lists the dues outstanding from the customers bucketed as per number of days due. This report is reviewed by the Finance Head and provisions are made for bad and doubtful debts in the books of accounts as per Company policy.
- Compliance purposes

The above examples give an idea as to how management of an entity depend on reports from the ERP systems that also have a bearing on the financial reports. These same reports are also used and relied upon by the Auditors during the course of the audit. This information is used by the Auditors via their audit opinion to provide assurance to other stakeholders on the integrity of the data.

Thus there is a need to test the reports from the ERP systems and applications relevant for financial reporting.

5.2 Types of Reports

There could be approximately 3 types of reports that can be extracted from ERP systems. The purpose for which these reports may be used are for analysing Financial or Operational data. These reports may also be used as part of statutory filing / compliance with SEBI, ROC, etc.

1. **Standard Reports –** These are reports that are available at the time of implementation of the ERP systems by the entity. These reports are inbuilt into the systems. Each ERP comes with a set of reports that can be used as is, if the company has implemented the ERP without too many modifications.

   This means that the Company is following the pattern of the Chart of Accounts, etc. as defined in the ERP and have not modified them. Thus if they stay within the parameters as defined in the ERP, these standard reports can be used without any modifications. In the below table, Company 1 can use the Standard Reports.

   For example: Purchase Register, Sales Register, Fixed Asset Register, Cash Flow statement etc.

2. **Customised Reports –** These reports are created by the entities with respect to their businesses, revenue streams, divisions etc.

   Here, the company has followed their own pattern or code for Chart of Accounts (CoA), Vendors, Customers etc.

   For example: B/S, P&L account etc. Alternatively the examples mentioned above such as Purchase/Sales/Fixed Assets Register can also be developed for the company specifically. These can be categorised as Customised reports.

Both the above types of reports are configured/coded and reside in the ERP systems.

COMPANY 1			COMPANY 2	
Sr. No.	**Details**	**Codes used as given when ERP implemented**	**Details**	**Codes as configured by Company at the time of implementation**
1	**2**	**3**	**4**	**5**
1	CoA including Vendors, Employees, Customers etc.	1000001 to 9999999	CoA	Control Accounts 100000 to 999999
			Vendors	VE100001 to VE110000
			Employees	EP0001 to EP999999
			Customers	CS100000 to CS 999999

Fig No. 5.2.1 Customised Reports

Thus, in Column 5, the Company 2 has followed its own model of defining CoA, Vendor codes, Employee codes, Customer codes etc. Thus the Standard reports based on CoA as defined in Column 3 cannot be used. The company will have to define its own TB, P&L account, B/S, Cash Flow statement etc. Such reports are called **Customised Reports.**

3. **Database queries / Other tools etc.**

Queries are used to retrieve information or data from a database in a readable format using a SELECT statement.

For example: database queries can be used to extract payroll information from a payroll database such as leaves available per employee, blank PAN details of employees who have not submitted PAN etc. These are converted into Excel spreadsheets etc. and used as reports.

5.3 Validation of Reports – Accuracy of Logic, Completeness and Accuracy of Data

In this session we shall understand the procedures to validate/test the reports. These procedures will be specific to the ERP/system implemented by the audited entity.

As per the Guidance Note, the three elements for determining the testing strategy for reports are to understand:

- Source Data
- Report Logic
- Report Parameters

At the start of the audit process, the auditor along with the auditee have to make a list of all relevant reports used by the company and the purpose for which they are used. The auditor will also have to understand the risks involved with each report.

- For example: if there is a mistake/error in the report, what is the potential impact on the business and the audit procedure? How frequently are changes made to the report
- Complexity of the report in terms of how are the values populated, number of formulae etc.
- Target audience of the reports – Senior Management, Staff etc.

Before the auditor plans to understand the types of reports and the procedures to validate them, it is necessary to check the integrity of the data within the system. The auditor has to:

- Test the General Information Technology controls (GITC's) within and surrounding the ERP systems.
- Test the controls within the business processes including sensitive access and segregation of duties etc. within and surrounding the systems. This is the source data for the reports.

This will give a reasonable indication to the auditor on the integrity of the data within the system. The results of the above mentioned procedures will determine the extent and type of procedures to be used to validate/test the reports for completeness and accuracy. There can be 2 scenarios pertaining to the results of the procedures:

- If the controls in GITC and Business Processes are found to be effective then the auditor may limit himself to performing certain tests on the reports.
- If the controls are found to be ineffective, the auditor will have to perform more detailed and substantive procedures. These procedures will be specific to the conditions relevant to the entity.

We shall talk of the procedures to test these reports later in this session.

The auditor as a first step need to understand the different types of reports that can be extracted from ERP systems/applications.

NOTE:
The company may have implemented a control on Quarterly Review of Aging Analysis by Finance Controller.
In such a scenario, the auditor will have to test 2 aspects of the control:

1. The Review by the Finance Controller
2. The integrity of the report. The procedure mentioned above can be used to test the integrity of the report. Here the timing of the extraction of the report becomes important. The auditor will also have to check whether the Finance Controller has reviewed the relevant latest report. The same report has to be independently extracted by the auditor and tested.

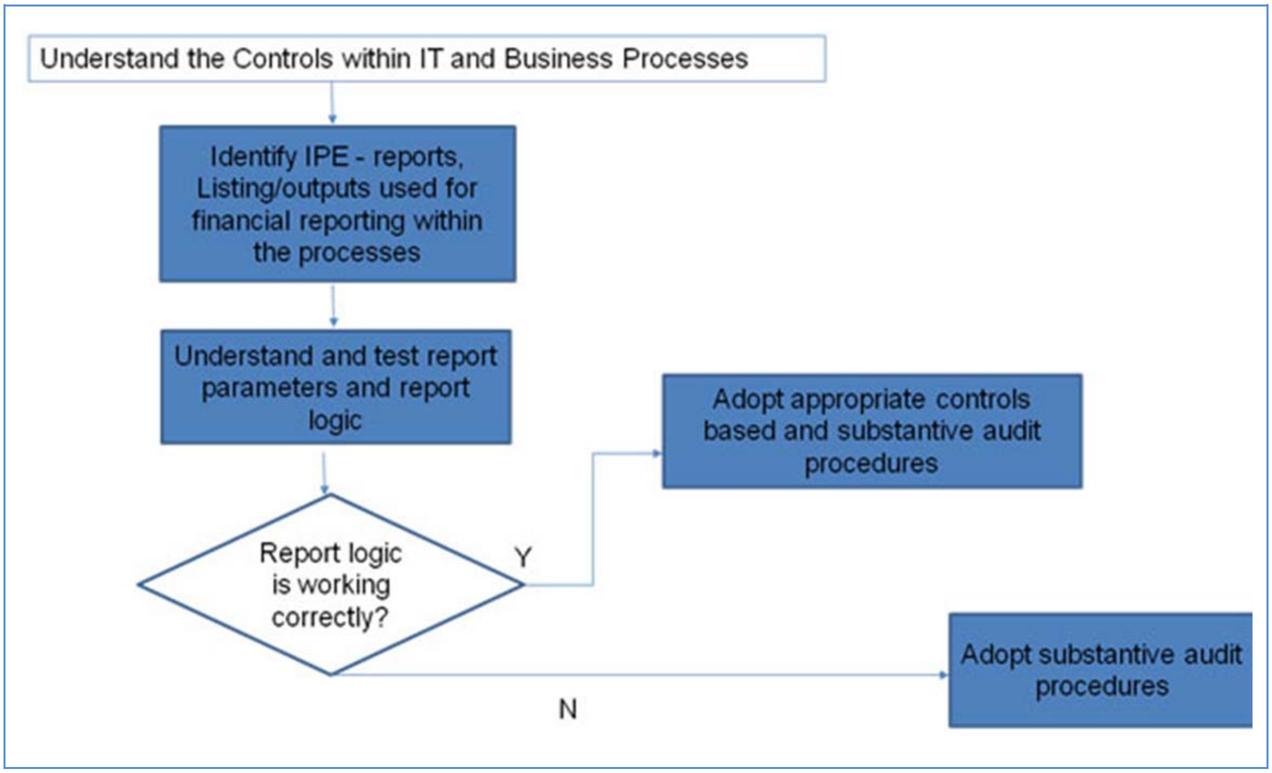

Understand the Controls within IT and Business Processes
Identify IPE - reports, Listing/outputs used for financial reporting within the processes
Understand and test report parameters and report logic
Report logic is working correctly?
Y
Adopt appropriate controls based and substantive audit procedures
N
Adopt substantive audit procedures

Fig. 5.3.1 implemented a control on Quarterly Review of Aging Analysis

5.3.1 Standard Reports

5.3.1.1 1st year of audit of the entity:

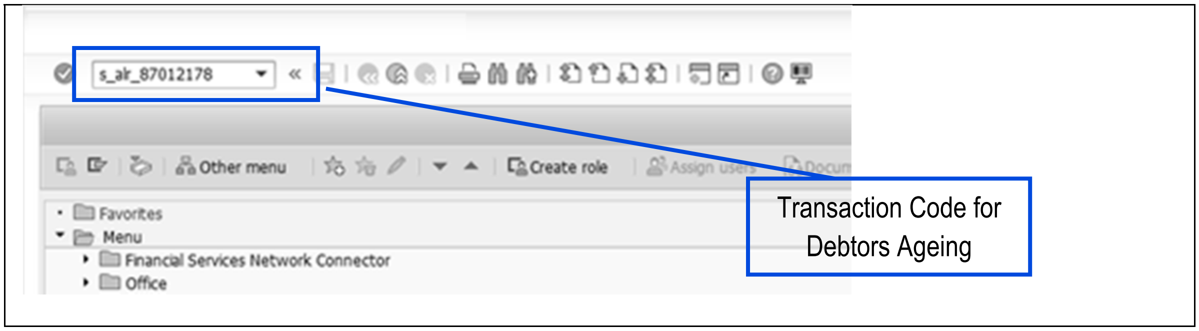
For example if the company has implemented SAP, the auditor may take steps as mentioned below:

Example 1: Debtors outstanding statement

Assumption – The results of GITC and Controls in business process testing are positive and reliance may be placed on them. Access to add/modify/delete these reports are restricted and changes to the reports are authorised.

- The company uses the following indicative commands in SAP to generate reports:
  (a) se16
  (b) se16n
  (c) sa38
- The auditor should ensure with the IT personnel whether there has been any change to the program code of the said report. In a case of a standard report, the creator/modifier of the report would be the vendor i.e. SAP themselves. The auditor can take a screenshot to ensure the same.

- If the evidence found in the change management logs indicates that the vendor - SAP was the last user to access the report at the time of implementation of the ERP.

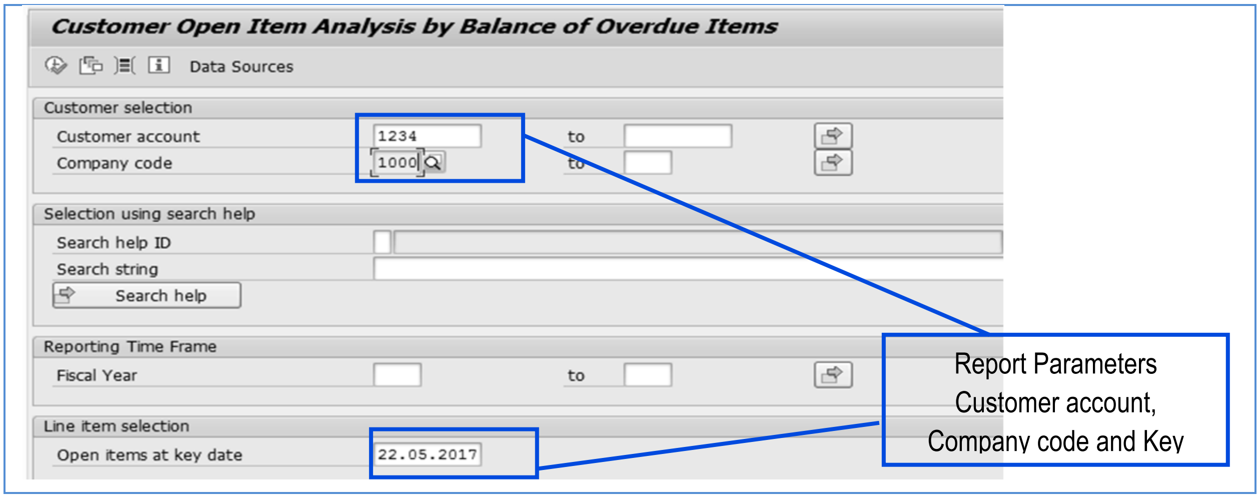


s_alr_87012178

Transaction Code for Debtors Ageing

Fig. 5.3.2 Debtors outstanding statement

Report Parameters:



Customer Open Item Analysis by Balance of Overdue Items

Customer selection

Customer account 1234 to

Company code 1000 to

Selection using search help

Search help ID

Search string

Reporting Time Frame

Fiscal Year to

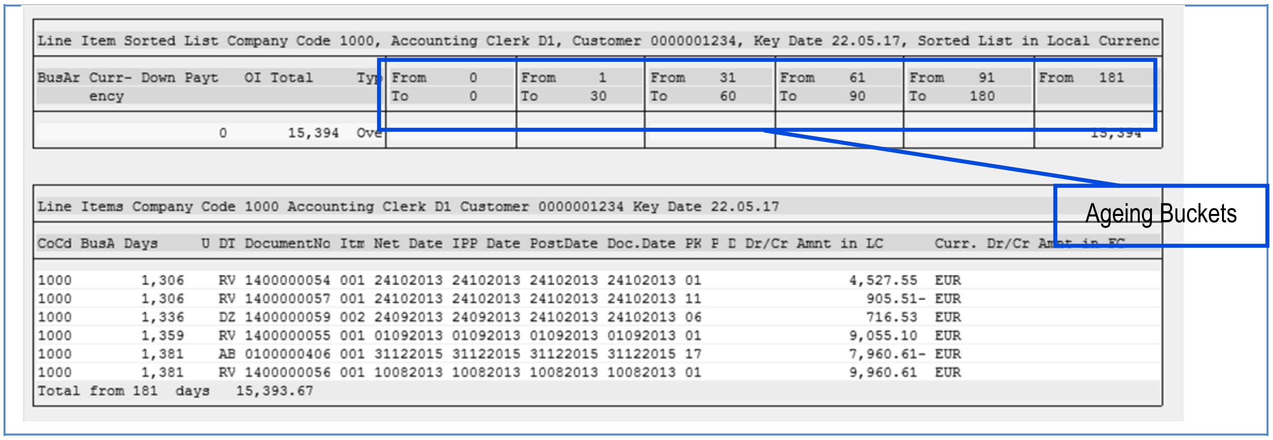
Line item selection

Open items at key date 22.05.2017

Report Parameters Customer account, Company code and Key

Fig. 5.3.2: Report Parameters

Report Output:



```
Line Item Sorted List Company Code 1000, Accounting Clerk D1, Customer 0000001234, Key Date 22.05.17, Sorted List in Local Currenc

BusAr Curr- Down Payt   OI Total     Typ From      0  From      1  From     31  From     61  From     91  From    181
      ency                               To        0  To       30  To       60  To       90  To      180

                    0       15,394   Ove                                                                   15,394

Line Items Company Code 1000 Accounting Clerk D1 Customer 0000001234 Key Date 22.05.17

CoCd BusA Days      U DT DocumentNo Itm Net Date IPP Date PostDate Doc.Date PK P D Dr/Cr Amnt in LC      Curr. Dr/Cr Amnt in FC

1000         1,306    RV 1400000054 001 24102013 24102013 24102013 24102013 01                 4,527.55  EUR
1000         1,306    RV 1400000057 001 24102013 24102013 24102013 24102013 11                   905.51- EUR
1000         1,336    DZ 1400000059 002 24092013 24092013 24102013 24102013 06                   716.53  EUR
1000         1,359    RV 1400000055 001 01092013 01092013 01092013 01092013 01                 9,055.10  EUR
1000         1,381    AB 0100000406 001 31122015 31122015 31122015 31122015 17                 7,960.61- EUR
1000         1,381    RV 1400000056 001 10082013 10082013 10082013 10082013 01                 9,960.61  EUR
Total from 181   days   15,393.67
```

Fig. 5.3.3: Report Output

- The auditor needs to then understand and test the completeness and accuracy of the report. The debtor's outstanding statement will have various buckets or columns. The buckets could be Upto 30 days, 31-60 days, 61-90 days, 91-180 days and Above 180 days, depending on the date of invoice which is outstanding.

  For example: Debtor 1

  The auditor can devise a procedure to take one transaction – one sample per scenario. In this case, one invoice per bucket as a sample is to be tested. Since these transactions are automatically populated in the report, if the tests pass for one transaction, then the same inference can be made for other transactions too.

- The original hard copy of the Invoice can be compared with the entry in the Outstanding statement for the following fields: Date/Invoice no./Customer name/Amount etc. If the values match between the original Invoice and the details in the Outstanding statement, the accuracy assertion is established.

- To establish the completeness assertion, the Grand Total of the Outstanding statement for all Debtors can be compared to the total of the value of Debtors appearing in the B/S or TB or can be checked on the screen itself.

Once the values are found to be matching, then a decision to rely on the report can be taken.

The above example pertained to SAP. Even in other ERP's/tools/manual reports, the Company may be using reports as given below. In this scenarios, testing of such reports as mentioned above have to be performed.

Debtors Outstanding Statement							
Party Name	Invoice No.	Total	0-30 days	31-60 days	61-90 days	91-180 days	> 180 days
Debtor1	1						
	2						
	TOTAL A						
Debtor 2							
	1						
	2						
	3						
	TOTAL B						
	GRAND TOTAL A+B						

5.3.1.2 Subsequent years of the audit

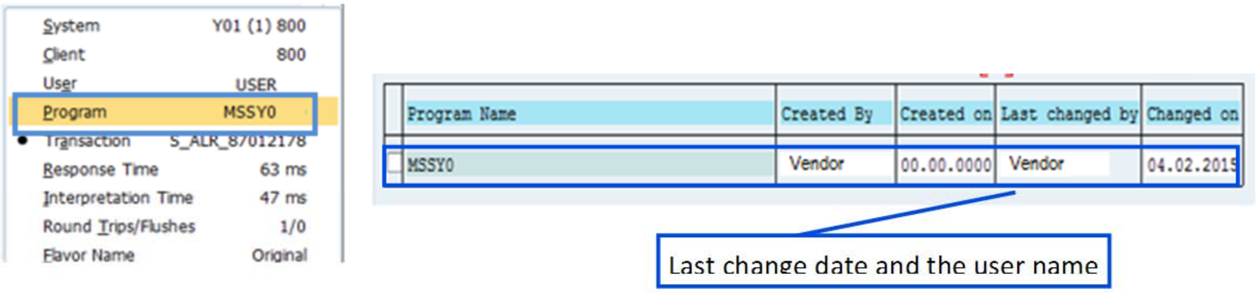
Assumption: The GITCs and relevant Business process controls are tested and found to be effective.

1. The auditor can test the creator/modifier value of the report and check if the value is the vendor - SAP as per results of the previous year. The auditor can take a screenshot to ensure the same. If there is no change in the values, no further testing need be done and reliance can be placed on the report.

Transaction code and the underlying program of the report

LAST CHANGE DATE AND THE USER W

HO HAS CHANGED:



System Y01 (1) 800
Client 800
User USER
Program MSSY0
Transaction S_ALR_87012178
Response Time 63 ms
Interpretation Time 47 ms
Round Trips/Flushes 1/0
Flavor Name Original

Program Name	Created By	Created on	Last changed by	Changed on
MSSY0	Vendor	00.00.0000	Vendor	04.02.2015

Last change date and the user name

Fig. 5.3.4:Last Change Date & the User Name

5.3.2 Customised Reports

As mentioned in the introduction, these reports are created by the business/IT persons in the company for their use and reporting requirements.

The same procedure as mentioned for Standardised reports need to be followed. The differences are:

1. While testing for users who have access to create/modify report, the auditor will have to verify whether the user names who have created/modified the reports are authorised users. If any change to the report has happened in the year of audit, then appropriate approvals should be verified.
2. The auditor has to follow the same test procedures to test for completeness and accuracy as mentioned above.
3. Unlike standard reports, the procedures to test the completeness and accuracy of the customised reports have to be performed every year.

Path:

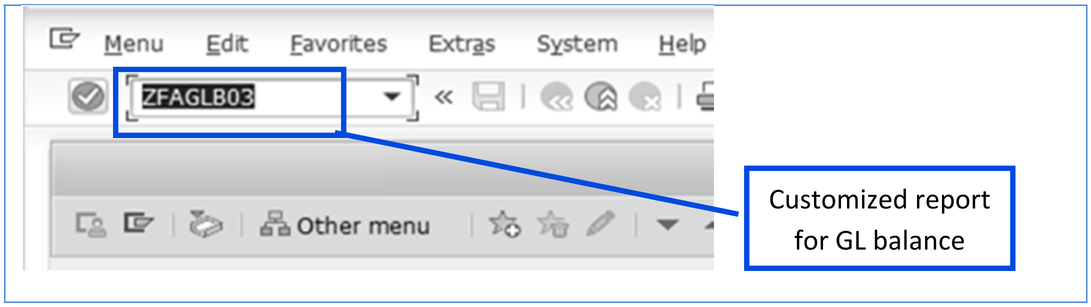
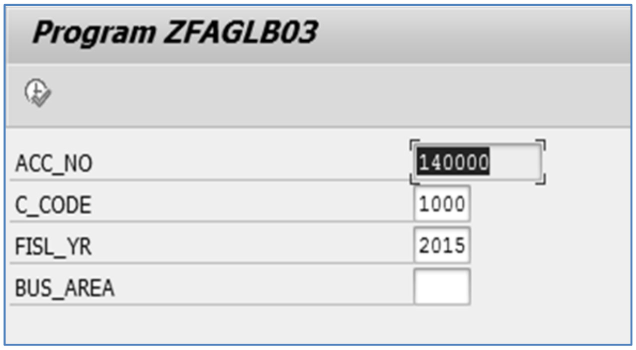


Fig. 5.3.5: Customised Report

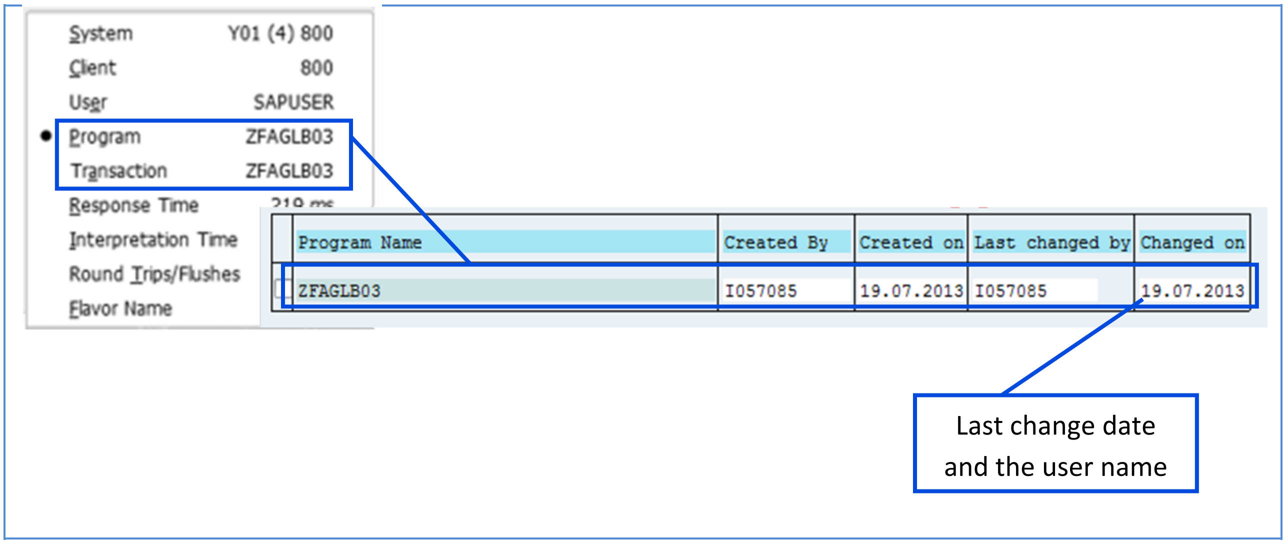
Report Parameters


Program ZFAGLB03

ACC_NO	140000
C_CODE	1000
FISL_YR	2015
BUS_AREA	

Fig. 5.3.6: Report Parameters

Underlying Program of the Report



System	Y01 (4) 800
Client	800
User	SAPUSER
Program	ZFAGLB03
Transaction	ZFAGLB03
Response Time	219 ms
Interpretation Time	
Round Trips/Flushes	
Flavor Name	

Program Name	Created By	Created on	Last changed by	Changed on
ZFAGLB03	I057085	19.07.2013	I057085	19.07.2013

Last change date and the user name

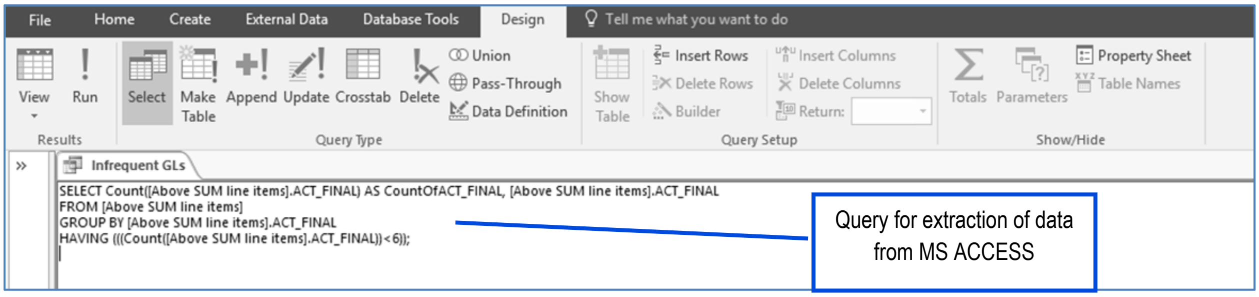
Fig. 5.3.6: Underlying Program of the Report

5.3.3 Database Queries/Other Tools

Since, these reports are extracted on ad hoc basis or on as and when basis, the auditor needs to adopt a more substantive approach to test the data extracted. Such reports have a high probability of the data being manipulated after creation.

For example, MS Access reports, excel sheets etc. come under this category.

For example, refer below the screenshot of a query in MS Access for extraction of infrequently used GL accounts for less than 6 times in a year.



```
SELECT Count([Above SUM line items].ACT_FINAL) AS CountOfACT_FINAL, [Above SUM line items].ACT_FINAL
FROM [Above SUM line items]
GROUP BY [Above SUM line items].ACT_FINAL
HAVING (((Count([Above SUM line items].ACT_FINAL))<6));
```

Query for extraction of data from MS ACCESS

5.4 Impact of conclusions of GITCs on Report testing

As mentioned in the earlier sections of this chapter, before we start to test the reports, the auditor needs to understand, evaluate and test the General Information Technology Controls (GITC's). The results of the GITC tests will have a bearing on the procedures to be followed to test reports.

Scenario 1: Controls in all domains of GITC's are effective and there are no relevant deficiencies.

In such a case, the auditor can follow the procedures as mentioned above to test the reports – both standard and customised.

Scenario 2: Controls are ineffective in all domains of GITC's

Therefore, the procedures to test the reports have to be different from the above mentioned. The auditor will have to devise a more substantive approach and other substantive procedures to testing the reports. The auditor cannot rely on just one sample to test the completeness and accuracy assertions of the report.

This will be further elaborated in the session on GITC's.

5.5 Timing of Report Testing

Deciding when to test a report is a critical element of the audit. Some of the criteria to be used to decide timing of report testing are:

1. The data captured by a report is also essential in deciding the timing to test a report.

   A report may capture real time data.

   For example in a telecom industry, reports may be used to for revenue assurance, value added services etc. Such reports may have values changing on a daily/monthly/quarterly/yearly basis. Hence, such reports have to be tested as per the frequency in which they are used. If the auditor delays testing the report, the values may be outdated and the results may not be accurate.

2. Company policy – If a report is generated and used by a Company on an annual basis.

   For example Provisions made on obsolescence of inventory. The report is reviewed and entry is made in the books of accounts as per this report. The auditor will also have to test a report as per the frequency used by the company.

3. There may be instances where the company has implemented a new ERP during the financial year. The legacy/older ERP is no longer used. The auditor may have to test the reports in both the systems as per the frequency of the report.

   For example, the company has implemented a new ERP from October 1st. They have a control of review outstanding debtors and provisions made in the books of accounts every quarter. If the auditor decides to test for 2 quarters - In such a scenario, the auditor may have to test the reports in both the systems.

4. Another important factor to be considered is the inclusion of Period end entries. The auditor will have to understand the type of entries passed and whether they are included in the logic of the reports.

5.6 Conclusion of Impact of Deficiencies in Report testing on audit

The auditor may be faced with a situation where there are deficiencies in the reports/IPE that have been tested. The errors at a minimum may be of 2 types:

- Logic errors
- Arithmetical errors

o As per the scoping details, these reports are used by the Company and relied by the auditor during the audit process. Hence these reports are tested by the auditors.

Thus, the auditor will have to accordingly coordinate with the company to make them understand the deficiencies found and check if they have rectified the report/IPE. The auditor will have to modify their audit procedures to calculate the impact on the financial statements. Also, the auditor will have to independently obtain the information from the company’s ERP for the purposes of their audit.

Example 1:

The debtors ageing statement given in Section 3 of this session:

All the details such as Invoice number, Party name, Amount etc. are correctly appearing in the name. However, the ageing buckets to calculate the number of days outstanding of the invoice is calculated from the due date of payment of invoice. This is wrong as the date has to be calculated from invoice date.

In such a scenario, the auditor will have to ask the company

o to create a new report or

o calculate the ageing correctly in the same report.

Accordingly the provisions etc may undergo a change in the financial statements.

Example 2:

In the same debtors ageing report, the outstanding buckets along with other details such as Invoice no. name of party, Date etc is appearing correctly. However, there are arithmetical errors. The total of all the buckets are not totalled correctly.

This can be verified by taking the Grand total of the Debtor ageing statement and tallying it with the total in the Trial Balance.

In both the above scenarios, the auditor will have to adopt appropriate substantive procedures to test the data.

5.7 Exercise

1. Which of the following method is used to produce reports about data.

    (a) Standard Reports

    (b) Customised Reports

    (c) Database queries.

    (d) All of the above

2. SELECT statement is used to generate which type of reports:

    (a) Standard Reports

    (b) Customised Reports

(c) Database queries.

(d) None of the above

3. The auditor may limit the test procedures to test reports when

(a) Controls in Business process and GITC are effective

(b) Controls in Business process are effective and GITC are ineffective

(c) Controls are ineffective

(d) None of the above

4. What are the factors to be considered for timing of report testing:

(a) Quality and type of entries

(b) Company Policy

(c) Implementation of new systems

(d) All of the above

5. Some of the reasons to test reports by auditors:

(a) Used by management to take decisions

(b) Used by auditors as part of audit

(c) Used by management for compliance purposes

(d) All of the above.

6. Prior to testing of reports, the auditor needs to understand, evaluate and test the ________ and _______.

7. On the assumption that the GITC's are effective, the auditor needs to follow which sampling procedure to test a report:

(a) One transaction

(b) One transaction per scenario

(c) Appropriate substantive procedures

(d) None of the above

8. The GITC's are effective and a report has been tested in earlier years. In subsequent years, the auditor may adopt an approach of testing ______________ of the report.

9. The 2 assertions generally evaluated at the time of testing reports are ______________ and __________.

10. System Reports which are used to analyse business operations and are extracted from systems not relevant for financial reporting, need not be tested.

(a) True

(b) False

5.8 Case Study

Access Limited is Private Limited Company. It is using SAP as its main ERP. The Company at the time of implementation of ERP decided to use only the Purchase and Sales Register as given by SAP. The IT team of Access Ltd along with the Finance team created a customised report for Debtors Aging Statement. However, it decided to prepare the P&L and Balance Sheet outside the system in MS Excel.

This is the second year of audit of Access Ltd. You are in the audit team and have been given the task of testing the reports as part of the Audit of Financial Statements. Devise a testing strategy to test these reports. The GITCs have been tested and found to be effective.

ANSWER TO EXERCISE

1. Correct answer is d: All of the above

   All the 3 types of reports – Standard, Customised and Database queries are methods to extract data or Information from the systems.

2. Correct answer is c: Database queries

   Database queries using SELECT statement is commonly used to generate data. Standard reports and customised are generated using pre-existing commands or menu paths in the ERP.

3. Correct answer is a: Controls in Business process and GITC are effective

   When the controls are ineffective either in Business Processes or GITC then one of the elements of determining testing strategy is affected namely source data.

   Thus, controls in Business process and GITC have to be effective for the auditor to consider specific test procedures.

4. Correct answer is d: All of the above.

   The company may have period end entries to be passed. Another scenario could be that the company has implemented a new system. Hence reports in both the systems may have to be tested for different periods. Also, the company may have a policy for provisions for debts, obsolescence etc. Hence, all the criteria have to be considered to determine the time to test reports.

5. Correct answer is b: Used by the auditors as part of the audit

   The reports which the auditors use as part of the audit need to be tested. This list may also include reports used by the Management.

6. Correct answer is General Information Technology Controls and Business Process Controls

7. Correct answer is b – One transaction per scenario.

   In the case of Debtors outstanding statement, if there are various buckets depending on the number of days outstanding of the invoice, one transaction per bucket has to be tested.

8. Correct answer is Last change date

9. Correct answer is Completeness and Accuracy

10. Correct answer is True. If a system is not relevant for financial reporting, then reports from that system need not be tested.

5.9 Answer to Case Study

Report Testing Strategy for second year of audit.

Standard Reports – Purchase and Sales Register -

- Ascertain from last year audit work papers if there were no issues in testing these reports.
- If so, test the Last change date of the report.
- If no change from previous year, no further testing required.

Customised Reports – Debtors Ageing Statement

- Take one sample per bucket and reconcile with original documents/evidences.

Excel Reports – P&L account, Balance Sheet

- To be tested by using appropriate substantive procedures.

5.10 References and Further Reading

1. Standards on Auditing published by the Institute of Chartered Accountants of India (ICAI), www.icai.org > Resources
2. Guidance Note on Audit of Internal Financial Controls Over Financial Reporting issued by Auditing and Assurance Standards Board. - (14-09-2015), www.icai.org
3. Companies Act 2013, www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf

5.11 Glossary

ERP – Enterprise Resource Planning

ROC – Registrar of Companies

IPE – Information Produced by the Entity

GITC – General Information Technology Controls

CHAPTER

6

NEW SYSTEMS AND DATA MIGRATION REVIEW

LEARNING OBJECTIVES

- To understand about new systems implementations
- To understand the data migration strategy and approach in an ERP environment
- To understand how to review new system implementations and data migrations
- To understand how to determine and evaluate impact of deficiencies in data migrations on overall audit

6.1 New Systems and System Upgrades (Functional Vs Technical)

Enterprise resource planning (ERP) is a company-wide integrated computer software system used to manage and coordinate all the resources, information, and functions of a business from shared data sources. ERP delivers a single database that contains all data for the software modules, which include Sales, Purchase, Materials Management, Human Resource & Payroll, Finance & Accounts, etc. Every ERP will have their own terminology to map business process to software modules. For example, in SAP the purchase and inventory processes are provided in the module known as Materials Management the same processes in Oracle are known as Procurement and Inventory.

Some of the reasons why companies consider implementing a new ERP system or migrating from existing legacy systems to ERP are as follows:

- To enable growth in business
- Take advantage of technology to carry out business faster and accurately
- Centralisation of data for better reporting and MIS
- Implement automated controls and enhance internal controls
- increase the level of automation in business process and increase operational efficiencies
- to respond to changes in business environment including regulatory changes
- obsolescence of existing technology or older versions are no longer supported by system vendors
- Outsourcing of business process to a third party

With the pace and frequency of changes in the overall business environment increasing periodically, the need for migrating systems has also become more common. The following scenarios may exist when systems are being implemented or migrated.

- Implementation of a completely new accounting system or ERP. For example, Tally, Quickbooks, In-house developed ERP or SAP
- Migrating from an existing system to a new ERP. For example, Tally/Quickbooks to SAP
- Migrating from an existing system to an enhanced version of the same system. For example, SAP 4.7 to SAP 6.0, Oracle 11i to Oracle R12
- Technical migration where the IT infrastructure including operating system, database, network or hardware are changed but no change in version or functioning of ERP.

  For example, the existing Windows 2008 R2 Server, on which the ERP is installed, is migrated to a newer Windows 2016 Server operating system and all the desktop operating systems in the company are upgraded from Windows 7 to Windows 10. In this example, the business functionality of ERP does not change and hence it is considered as a technical migration.
- Implementing new modules in an existing ERP. For example, Payroll module is implemented in an existing ERP where other modules viz., Finance & Accounts, Sales, Purchases and Inventory are already operational.

The auditor needs to understand well in advance any plans a company may have to undertake major changes in the IT environment during an audit period. The auditor has to consider the possibility of auditing in two very different IT environments in the same year and should assess risks accordingly. Some of the areas where a migration could impact audit include the following:

- Change in understanding of existing business process
- New risks could arise
- Activities and existing controls could undergo a change
- More automated controls are likely to be implemented
- User access rights and segregation of duties could change
- Reports and system generated data i.e., information produced by entity (IPE) could change
- Considerations for outsourced activities

6.2 Data Migration Strategy

ERP migrations are similar to any other project and accordingly the auditor should understand the strategy and approach that is being adopted in a particular migration project. The key phases in any ERP migration project will consist of the following as shown in Fig 6.2.1:

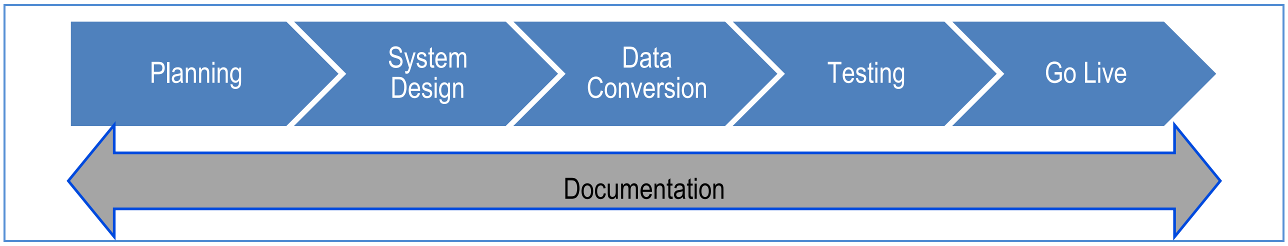


Fig 6.2.1: Data Migration Strategy

Planning: In this phase of migration the objectives of migration and the migration strategy are defined. Commitment and involvement of top management is defined and an individual who will be the business sponsor is identified to take key decisions. Team is formed and roles and responsibilities are assigned. A budget for the migration is allocated. Key dates, timelines and milestones are determined. A risk assessment carried out and critical dependencies - including availability of staff for the migration project, support from vendors and external consultants, readiness of IT environments, etc. - are identified upfront. Back-out and rollback procedures are planned as a contingency measure.

System Design: In this phase of migration the AS-IS (existing) system and process is understood and the TO-BE (proposed) system and process prepared including the process flows, data flows and business process re-engineering. Configuration and Customisations required are determined and the codification is prepared. Interfaces with other systems and applications are determined.

Data Conversion: In this phase of migration involves identification of source data, data mapping between source(existing) and target (proposed) systems is defined including the development of automated data extraction and transfer programs or scripts. Intermediary data stores called staging areas are used to hold, convert and transfer data. Inconsistencies in data, incomplete and inaccurate data are identified and corrected as part of data cleansing and data enhancement. Integrity checks are done to ensure completeness and accuracy of data. Mock conversions are carried out iteratively to rectify errors and data inconsistencies.

Testing: In this phase of migration various levels of testing are carried out that include, unit testing, integration testing, user acceptance testing. Test cases, scenarios and test scripts are prepared to test the functionality of the new system.

Implementation (Go Live): In this phase of migration the team checks if all objectives of migration and the migration strategy are achieved. Any deviations should be identified and resolved. Adequate training has been provided to the user of the new system. Assurance should be obtained from an independent auditor prior to implementation in the form of a pre-implementation review report. A representative of top management should provide approval for Go live and communicate to all stakeholders about the launch of new system. A rollback plan is defined as a contingency measure in case migration is not successful.

Documentation: For all phases and migration activities, relevant documentation should be prepared and signed off by the project team.

The below illustration is an example of a high-level ERP Migration Plan as shown in Fig 6.2.2.

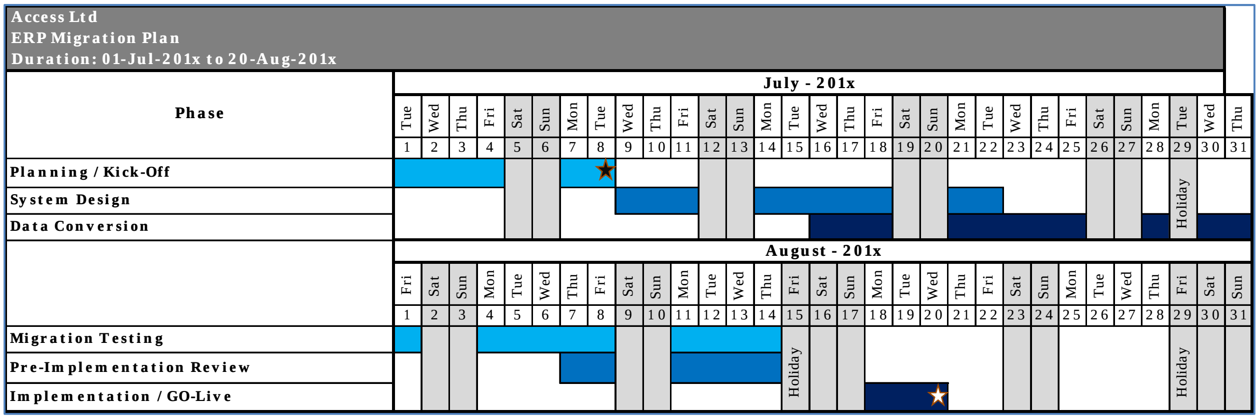


Fig 6.2.2: High Level ERP Migration Plan

It should be noted that the migration strategy could vary from company to company and depends on the scope and nature of migration i.e., technical or functional. The auditor should obtain an understanding of the scope and nature of migration to assess impact on audit.

6.3 Masters, Balances, Line-items, Open items

When planning a migration from an existing system to a new system, some of the important considerations include determining an approach for migration of existing master data, historical transaction data, open items and account balances.

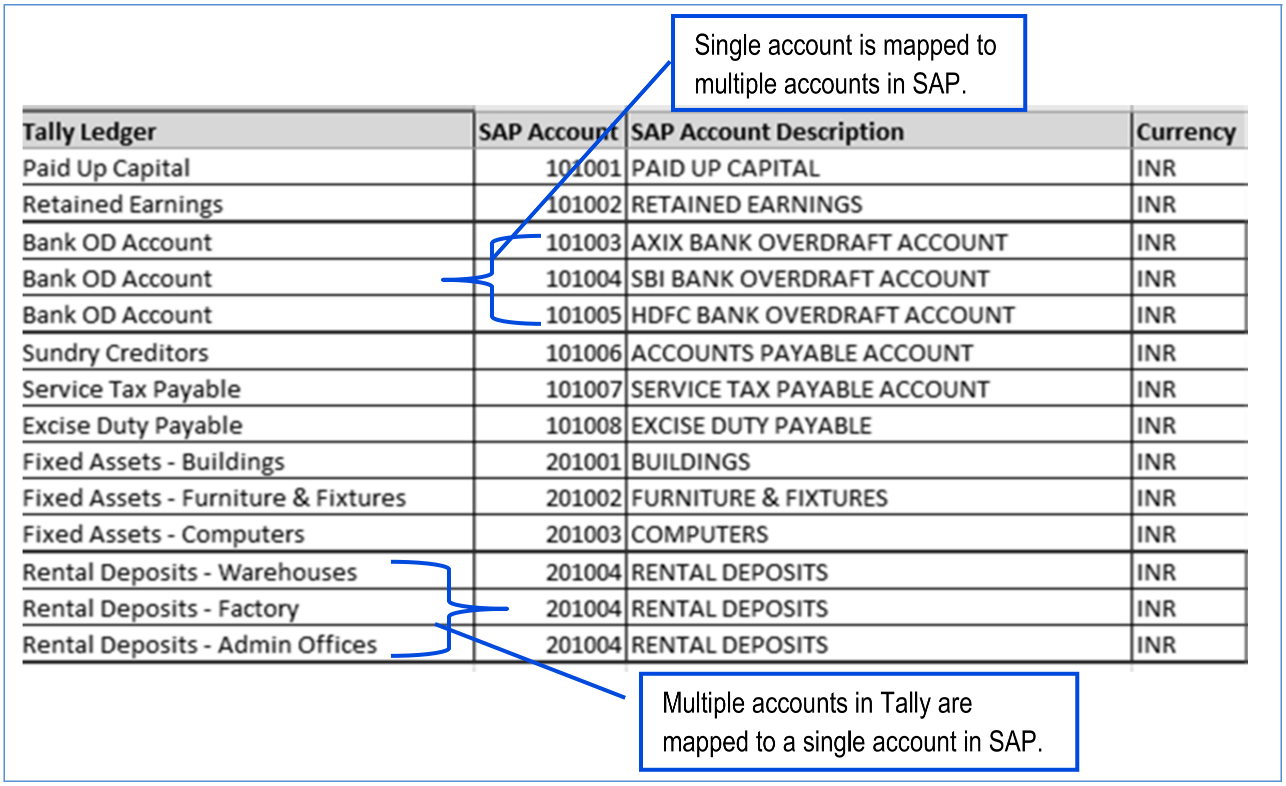
A migration project provides an opportunity to review and carry forward only the relevant data and discard obsolete data. The likely scenarios may be as follows:

- Duplicate master data is identified and blocked
- Obsolete or dormant master data is blocked
- Only current price masters are carried over to new system OR revised prices with effect from Go live date could be adopted
- Missing fields, additional fields, mandatory fields in new system are identified and updated. Additional data that is presently not available may have to be obtained from the respective source viz., customer, vendors

For migrating the financial data and account balances, the following scenarios can be considered.

- Definition of new chart of accounts
- Mapping the legacy and new charts of accounts. See illustration for examples of one-to-many and many-to-one GL mappings
- Closing balance in the legacy system is carried over as opening balance in new system
- Opening balances are directly entered or uploaded in new system OR processed through temporary migration accounts as accounting entries for better control.

Sample Chart of Accounts Mapping – Tally to SAP



Single account is mapped to multiple accounts in SAP.

Tally Ledger	SAP Account	SAP Account Description	Currency
Paid Up Capital	101001	PAID UP CAPITAL	INR
Retained Earnings	101002	RETAINED EARNINGS	INR
Bank OD Account	101003	AXIX BANK OVERDRAFT ACCOUNT	INR
Bank OD Account	101004	SBI BANK OVERDRAFT ACCOUNT	INR
Bank OD Account	101005	HDFC BANK OVERDRAFT ACCOUNT	INR
Sundry Creditors	101006	ACCOUNTS PAYABLE ACCOUNT	INR
Service Tax Payable	101007	SERVICE TAX PAYABLE ACCOUNT	INR
Excise Duty Payable	101008	EXCISE DUTY PAYABLE	INR
Fixed Assets - Buildings	201001	BUILDINGS	INR
Fixed Assets - Furniture & Fixtures	201002	FURNITURE & FIXTURES	INR
Fixed Assets - Computers	201003	COMPUTERS	INR
Rental Deposits - Warehouses	201004	RENTAL DEPOSITS	INR
Rental Deposits - Factory	201004	RENTAL DEPOSITS	INR
Rental Deposits - Admin Offices	201004	RENTAL DEPOSITS	INR

Multiple accounts in Tally are mapped to a single account in SAP.

Fig 6.3.1: Sample Chart of Accounts Mapping – Tally to SAP

Historical transaction data including orders, invoices, goods receipt and dispatch notes and other standard and non-standard journal entries may not be migrated to new system and will most likely remain in the legacy system. The implications of this need to be considered from the following points of view

- Legal and statutory requirements including maintaining books of accounts in accordance with Companies Act 2013
- Availability of records for tax audit and assessments.
- The duration for which books of accounts and records are required to be maintained in legacy system
- Access controls for the legacy system
- Protection of legacy data from being changed
- Software license terms of use for legacy system including application, operating system and database

Open items could exist as on the day of migration and it is important that the migration approach should envisage and factor for such open items. Open items could exist the following scenarios

- Open orders – purchase, sales and production orders
- Open invoices – vendor, sales invoices

- Advances – received and paid
- Loans to employees
- Stock-in-transit
- Depreciation history and accumulated depreciation for fixed assets.

The auditor should understand the approach adopted by the company management to assess the impact on audit.

6.4 When to Test?

Having obtained an understanding of the migration approach, the business environment and the IT environment, the auditor should perform a risk assessment for each phase of the migration process and identify the risks that could impact the audit. The auditor should design appropriate audit procedures that include evaluation of controls that are in place to mitigate the risks. The auditor should test these controls for design and operating effectiveness.

The testing for data migrations can be performed pre-implementation which means either immediately preceding the Go live phase, when a substantial part of the migration has been completed, or post-implementation meaning after the Go live phase. The suggested approach is to perform both pre-implementation and post-implementation reviews because of the following reasons

- a pre-implementation review provides an opportunity for the company to identify gaps, if any, in the migration process and address the same in a timely manner.
- a pre-implementation also provides early assurance on the migration process and controls which can be useful in planning other audit procedures better.
- a post-implementation review provides assurance on the effectiveness of migration process and controls. However, in case of any gaps or deficiencies that are identified there is no opportunity to address and remediate these gaps. The auditor should evaluate and report the gaps and deficiencies and design further audit procedures, if necessary, in the same way as for other control deficiencies.

It should be noted that pre-implementation or post-implementation reviews can be carried out as separate non-audit engagements by internal audit or another third-party auditor depending on the company's requirements. In any case, the statutory auditor is still required to perform a review of migration process and controls as part of the audit process as part of testing General IT Controls, it is not an option. However, the auditor may consider using the work performed by internal auditors in accordance with guidance given in SA 610. Whether the auditor plans to rely on the work done by internal auditor or not, the auditor is required to evaluate and address the gaps and deficiencies, if any, that have been identified by the internal auditor/third party auditors.

The table below has examples of some of the risks and controls at each phase of the migration process that are relevant when implementing or migrating to new systems

Phase	Risk	Control Activity
Planning	Project may not go as per the plan.	Project manager prepares the detailed Project Plan which includes step by step activities involved, the key dates and milestones, budgets, team allocation, etc. This plan is approved by the Business Sponsor/Steering Committee.
System Design	Business process may not be accurately or completely mapped	As-Is and To-Be process document or Blueprint of existing business processes with the proposed processes is mapped and documented by System Analysts. This document is reviewed by appropriate functional team members and approved by the Project Manager, Business Sponsor/Steering Committee.
Data Conversion	Transaction data may not be uploaded accurately in to the new system.	Converted account balances, data counts and totals are compared with comparative data from legacy system to ensure the accuracy and completeness data conversion. Project manager reviews data conversion results and ensures that differences are identified and resolved in a timely manner. Results of data conversion is documented and approved by the Business Sponsor.
Testing	Configurations made in ERP may not be accurate/may not function as per the requirement	Unit testing and Integration testing is done by project team and reviewed by module leader and project manager. User acceptance testing is done by business users and approved by the respective process leads. Testing results are documented and approved by the Business Sponsor.
Go Live	Processing business transactions may be started in the new system even before migration if fully completed and objectives are not met.	The Project Manager ensures that all planned objectives have been met and new system is ready for use. A pre-implementation review is carried out by an independent auditor to provide assurance that migration process and controls are effective. The Business Sponsor/Steering Committee reviews the project status and the pre-implementation report. Business Sponsor gives formal approval to start using the new system.

6.5 Conclusion on Impact of Deficiencies on Audit

As noted in the previous section, it is likely that deficiencies will be found during a review of migration process. Examples of such deficiencies include:

(a) a documented migration strategy and plan is not prepared

(b) a formal sign-off for user acceptance testing has not been obtained

(c) errors in data conversion have not been rectified

(d) approval for go-live was not formally obtained

Having found deficiencies, the auditor should evaluate the impact of these deficiencies on the audit. For this evaluation, the auditor should consider the following:

- are there any alternate sources which can compensate for lack of structured documentation. For example, email communications, minutes of meetings, project folders and working papers.
- In case of errors in data conversion, the auditor should determine if the errors are specific to a particular set of transactions, business process or pervasive. Based on this assessment, the auditor may be able to limit further audit procedures. For example, if the data conversion errors pertain to 25 sales invoices, the auditor may test these specific invoices substantively.
- consider using CAATs to ensure completeness and accuracy of data. For example, the auditor can rebuild the trial balance by extracting all transaction as on conversion date separately from legacy and new system, summarise these transactions in ACL and compare net account balances. Ideally, there should not be any difference between the legacy and new system after factoring for changes in chart of accounts.
- determine the aggregate financial impact of the deficiencies and compare with materiality.

The above examples are some of the ways in which the auditor thinks through the deficiencies and assess impact on audit. Wherever necessary, the auditor may have to obtain additional audit evidence to address the risk of material misstatement.

6.6 Exercises

Multiple Choice Questions

1. Which of the following is example of an ERP,

    (a) SAP

    (b) Oracle R12

    (c) In-House developed

    (d) All of the above

2. Which of the following activity is part of the System Design phase of a migration,

    (a) Allocation of Budget

(b) Configuration

(c) Mock conversion

(d) All of the above

3. At which phase of the migration would rollback procedures be triggered, if necessary

(a) Planning

(b) Data Conversion

(c) Go-Live

(d) Migration Testing

4. Which of the following require specific considerations during a migration,

(a) User access and segregation of duties

(b) Open items

(c) Master data

(d) All of the above

5. When would auditors review migration process and controls,

(a) During Pre-implementation/Post-implementation reviews

(b) When reviewing General IT Controls

(c) Both A & B

(d) None of the above

Fill in the blanks

6. ___________ should be prepared and maintained for all phases of migration.

7. The auditor should evaluate the _______ of deficiencies identified in the migration process.

8. A ______________ review provides an opportunity for the company to identify gaps in the migration process and address the same in a timely manner.

9. The auditor may consider using the work performed by internal auditors in accordance with guidance given in __________

10. Interfaces with other systems and applications are determined during ____________ phase of the migration process.

True/False

11. When a pre-implementation review has been performed and the gaps have been rectified, the auditor is not required to evaluate and test controls in the migration process. (True/False)

12. The auditor should consider using CAATs when evaluating deficiencies in migration controls. (True/False)

13. Migration approach and strategy will be the same for all companies. (True/False)

14. Duplicate master data records should not be considered for migration from legacy to new system. (True/False)

15. After migrating to the new system, the data in legacy system can be discarded. (True/False)

6.7 Case Study

Access Ltd is in the business of manufacturing and selling of mobile phones. Revenue in FY17 is INR 100 Crore and expected to grow at over 30% per annum for the next three years considering the significant increase in demand for mobile phones.

Access Ltd is currently using SAP ERP for accounting, sales and purchases and inventory. In view of upcoming GST tax reforms, which will be effective mid of FY18, the company is in the process of upgrading the SAP system to meet the new requirements. The company is also implementing a cloud based SalesForce CRM solution which will be integrated to the SAP ERP system to drive the Marketing and Customer Relation Management activities.

You are the auditor of Access Ltd for FY18. Your task is to,

(a) Identify the systems at Access Ltd.

(b) Determine which system is relevant for audit and why.

(c) Think of three audit considerations that come to your mind because of the change in existing systems.

6.8 References and Further Reading

1. Standards on Auditing published by the Institute of Chartered Accountants of India (ICAI), www.icai.org > Resources.

2. Guidance Note on Audit of Internal Financial Controls Over Financial Reporting issued by Auditing and Assurance Standards Board. - (14-09-2015), www.icai.org.

3. Companies Act 2013, www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf.

6.9 Glossary

ERP – Enterprise Resource Planning

GITC – General Information Technology Controls

SA – Standards on Auditing

CAATs – Computer Assisted Auditing Techniques

MIS – Management Information System

IPE – Information Produced by Entity

ACL – Audit Command Language (CAAT Tool)

IT – Information Technology

CRM – Customer Relationship Management

GST – Goods and Services Tax

6.10 Answers to Excises

1. Correct answer is D).

   SAP, Oracle R12 and In-house developed are examples of ERP.

2. Correct answer is B).

   Allocation of budget happens in Planning phase. Mock conversion is part of Data Conversion phase.

3. Correct answer is C).

   Rollback procedures are defined in the Planning phase and triggered during the implementation or Go live phase, if necessary.

4. Correct answer is D).

   Approach for migration of user access and segregation of duties, open items and master data should be considered.

5. Correct answer is C).

   Auditors can evaluate and test migration controls as part of pre-implementation, post-implementation reviews or during while reviewing General IT Controls during audit process.

6. Documentation.

7. Impact.

8. Pre-implementation review.

9. SA 610.

10. Planning.

11. False.

    The auditor has to evaluate and test the remediated controls.

12. True.

    The auditor can assess impact of deficiencies by analysing data using CAATs.

13. False.

    The migration approach will vary from company to company depending on several factors including the scope and nature of migration.

14. True.

    Duplicate master data is identified and discarded as part of data cleansing during migration.

15. False.

Several factors should be considered including legal and statutory requirements before legacy system is discarded.

6.11 Answer to Case Study

(a) The two systems are SAP ERP and Sales Force CRM

(b) SAP ERP is relevant because the financial accounting and transactions are processed in SAP.

Sales Force CRM does not have financial data that and hence, not relevant from an audit point of view.

(c) Some of the audit considerations are as follows:

- Changes in the general ledgers and Chart of Accounts – new ledger codes for GST will be created
- Changes in transactions – invoice formats, tax calculations
- Master data updates – customer and vendor masters to be updated with new GST tax codes
- Changes in business process and internal controls, including automated controls
- Changes in IPE – new reports will be created, reporting formats will be new

CHAPTER

7

NON STANDARD JOURNAL ENTRIES

LEARNING OBJECTIVES

■ What are Non-Standard Journal Entries in ERP's

■ Process to identify Non-Standard Journal Entries

■ Process to ensure completeness of data

■ Identify Criteria for JE analytics

■ Software Testing for scripts

7.1 Overview

Companies use ERP's to record transactions. In most ERP's these transactions are automated based on the business process. In addition to the sub-leger entries that arise out of business processes, the companies may also pass journal entries that impact the financial statements. We shall now try to understand the different types of journal entries

- **Standard Entries –** These transactions pertaining to sales, purchases, inventory, rent, audit fees, AMC expenses, salaries etc. are subject to internal controls as defined by the company.
- **Non Standard Entries –** In addition to the automated entries, these entities also record nonrecurring, unusual transactions or adjustment entries in the ERP's. These entries may not be subject to the same level of rigour of the internal controls or may not have passed through any controls at all.

  These transactions could be manual in nature and may pertain **for example**:

  ✓ Estimates, impairments etc.

  ✓ Adjustments to amounts already reported in financial statements – combinations, reclassifications etc.
- **Top Up entries –** These are residing outside the books – for example in excel sheets etc. and may impact the financial statements.

  ✓ Inter company set off entries etc.

For the purpose of this session we shall concentrate on Non Standard Journal Entries (NSJE) only. SA 240 and **The Guidance Note on Audit of Internal Financial Controls Over Financial Reporting** in paragraphs 64,66,80,90, IG 4.4 and IG 5.6, IG 19.21 and IG 21.9 also talk about unusual transactions and the audit procedures to deal with them.

Before identifying the various type of journal entries – standard, non-standard and top up, the auditor will have to understand, evaluate and test the process of internal controls in place to pass such entries.

These entries may be passed throughout the year or more generally at the end of a financial period. There is a possibility that these entries may be passed through sub ledgers like purchase or sales. However, in this case, there may be a level of collusion required, which may be difficult.

Hence, such NSJE are generally directly passed in the General Ledger. There is a risk of management override of controls in passing such entries. In each entity, the level of this risk may vary, but the risk is present. The risk of management override may also lead to risk of material misstatement to fraud which is a significant risk. As a result, the audit procedures should be very robust and relevant to the entity that is being audited.

There is another key aspect to remember while auditing in ERP environment. Other entries – automated etc. will be supported by relevant printed documents. These NSJE's may exist only in electronic form directly in the General Ledger with no supporting physical documents.

7.2 Process to identify Non Standard Journal Entries

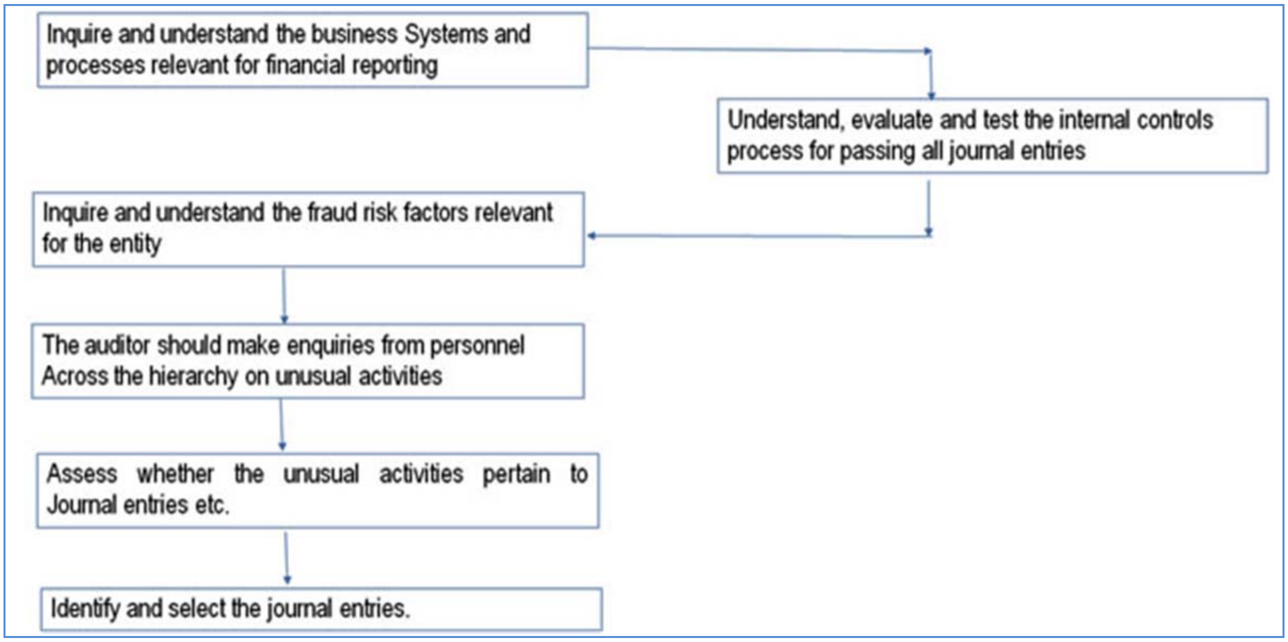

Inquire and understand the business Systems and processes relevant for financial reporting
Understand, evaluate and test the internal controls process for passing all journal entries
Inquire and understand the fraud risk factors relevant for the entity
The auditor should make enquiries from personnel Across the hierarchy on unusual activities
Assess whether the unusual activities pertain to Journal entries etc.
Identify and select the journal entries.

Fig 7.2.1 Process to identify Non Standard Journal Entries

The above process will assist the auditor in understanding the type of journal entries passed and more specifically Non Standard Journal Entries.

The points to note for understanding the business systems and processes are:

- Accounting software – ERP/customised/off the shelf packages
- IT team – in house/outsourced

- Type of entries – automated or manual etc.
- SA/SOD among IT and business teams etc.
- Timing of passing journal entries – end of day, weekend etc.

The points to note for understanding the fraud risk factors are:

- Sales targets to be achieved – important to investors, stock holders etc.
- Bonuses and incentives – employees
- Debt requirements – banks etc.

The auditor should generally ask open ended questions to the management to understand if there were any unusual activities during the year under audit.

- Whether the employee who recorded entries went on vacation and if there was a substitute during that period
- Whether the employee shared his user id and password with any person during the year.
- Whether any entries were passed during the year without any supporting documents.

Once the auditor gathers all the information, the assessment has to be made whether any of the replies received has translated to any journal entries. The criteria to be used to for selecting the non standard journal entries will be taken up later in this session. Prior to this, the population of journal entries have to be extracted and the completeness of data has to be ensured.

7.3 Process to ensure completeness of data

Once the auditor has completed his inquiries and gathered the requisite information, the next step is to understand the **timing of performing the journal entry testing**.

- Generally, the auditor will wait for the company to have passed most of the entries and closed the books of accounts for the period before deciding to take up the testing.
- Once the books are closed, even if the entries need to be passed, a register or a tracker is maintained on the further entries that may need to be passed.
- If the auditor decides to perform JE analysis before the year end, then the auditor along with the company will have to keep track of the entries passed subsequently and if required, analyse them later.

Once the auditor has decided to perform the journal entry testing, the entries need to be extracted. There are various ways of identifying journal entries passed in the system:

- If the journal entries are passed using a specific journal type then a list of such entries can be extracted from the system.
    - o **For example**, journal types could be MJV – Manual Journal Vouchers etc
- If the journal entries cannot be distinctly identified by the journal type, then the complete list of all entries are extracted. Out of this full list of entries, the auditor will have to identify journals for testing.

The process can be described as:

- **Extract the full list of entries.**
- **Perform completeness testing**
- **Based on understanding obtained from the company, identify the JE criteria to pick the Non Standard Journal Entries.**
- **Apply the criteria filter on the full list of JE entries**
- **Test the filtered list of Non Standard Journal Entries.**

7.3.1 Data fields to be extracted

Generally, some of the common fields for which data need to be extracted are given below. One point to keep in mind is that the ERP/application should have these fields and the company must be entering data in these fields for them to be extracted.

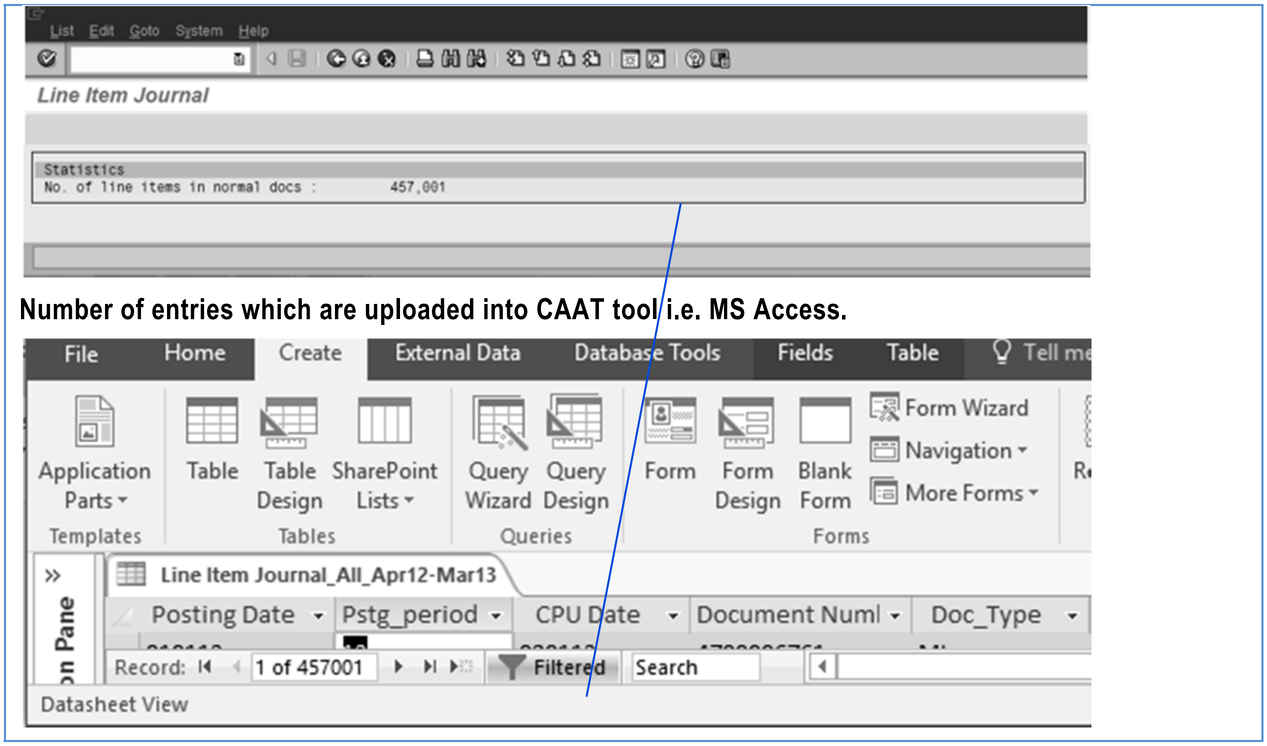
1. Date
2. Journal No.
3. Journal Type
4. Entry Date
5. Approved date
6. Posted date
7. Period
8. Business Unit
9. Account Number
10. Account Name
11. Description
12. Debit Amount
13. Credit amount
14. Line no.
15. Prepared by
16. Approved by
17. Posted by

7.3.2 Common methods to test for completeness of data:

Some of the common methods to test for completeness of data are:

- Roll forward testing – Roll forward the entries passed during the year to the balances in the Trial Balance. The auditor may use ACL/IDEA Caseware/MS Access/Excel to perform Roll forward testing
- Procedures other than Roll Forward Testing.
- **Roll Forward Testing**
    - **Using CAATS to test for completeness of data:**
        - Using tools such as ACL, IDEA Caseware, MS Access, Excel etc., the auditor can test the data for completeness.
        - Match the number of entries in the system with that extracted in the CAATS tool. Both the numbers should match.
        - Match the total number of debits with total number of credits for all the entries. The difference should be zero.

SCREENSHOT of number of entries in MS Access with system as shown in Fig 7.3.1



Line Item Journal

Statistics
No. of line items in normal docs : 457,001

Number of entries which are uploaded into CAAT tool i.e. MS Access.

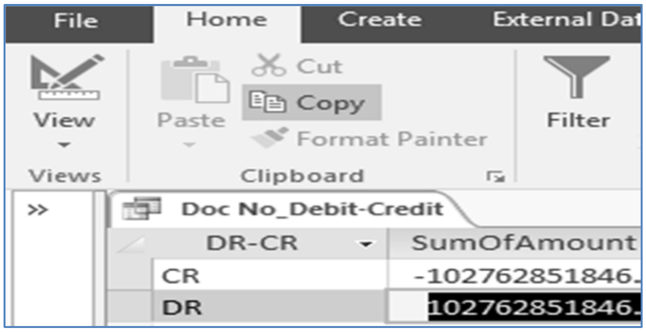
Line Item Journal_All_Apr12-Mar13

Posting Date | Pstg_period | CPU Date | Document Numl | Doc_Type

Record: 1 of 457001 Filtered Search

Fig 7.3.1 Number of entries in MS Access with system

SCREENSHOT of debits = credits as shown in Fig 7.3.2



DR-CR	SumOfAmount
CR	-102762851846.
DR	102762851846.

Fig 7.3.1 Debits=Credits

- If the company is using an ERP, then, the auditor can ask for a full list of entries based on Journal type and summarise the data based on Journal type. This can be reconciled with the Trial Balance and tested for completeness.

Journal Type	Amount
Sales	
Purchase	
Cash	
Total	

- The entries in the data extracted need to be match the highlighted areas.

Details	Opening balance	Debits	Credits	Closing Balance
Balance Sheet				
Cash balance	10000	2000	4000	8000
Profit & Loss				
Salaries	0	50000	2000	48000

- **Procedures Other than Roll Forward Testing**
  - There are industries/sectors where the roll forward testing may not be appropriate or feasible.
  - **For example** - in banks/financial institutions/e-commerce/retail sectors where the volume of transactions are huge, the auditor may have to think of a different method to test for completeness of data.
    - The auditor can identify the key account balances and perform roll forward testing only for those accounts and not for all accounts.

- There are high risk accounts such as - intercompany accounts and related party transactions the auditor can reconcile the opening balances and closing balances with previous year and current year financial statements and then test by roll forward the transactions (debit and credit).
- Holding company audits – A holding company with many subsidiaries - Journal entry testing may be very challenging. A possible path would be to adopt roll forward testing in the subsidiaries. At the holding company level, the auditor can test the consolidating and eliminating entries.
- CAATS can also help in finding out gaps in the sequence numbers of journal entries. This is useful where the volume of transactions are huge such as banks/financial institutions etc.
- CAATS can also help in finding out if there are duplicate journal numbers used.

7.4 Identify Criteria for JE Analytics

The auditor will have to know the business of the client and the industry and then decide on the criteria to be used for JE analytics. Some of the common criteria can be:

1. Seldom used accounts – Accounts that are used very infrequently.
2. Unusual combination of accounts –

a. Debit cash - Credit Revenue

3. Posted and approved by the same person
4. Persons passing entries or adjustments who generally do not pass entries
5. Unusual time of the day / on holidays/weekends etc.
6. Amounts having round numbers or same ending numbers

a. Numbers ending with 0000 or 9999 etc.

7. Small value entries but the volume of such entries are many.
8. Accounts that have significant estimates or period end adjustments
9. Accounts identified with risk of material misstatement
10. Entries passed after the books have been closed. Etc.

7.5 Software Testing of Scripts

The process of identifying NSJE and applying the JE criteria for testing is a long and time consuming process every year. Once the auditor understands the processes and controls in place to pass Journal entries, the type of journal entries, the information system (ERP) used to pass such entries etc., this process may be automated to build in efficiencies within the audit. The auditor need not spend time on operational matters. This will also assist the auditor in spending productive time performing the audit, analysing the data.

The auditor can take help from IT members in his audit team to develop a script whereby the data can be extracted.

- The auditor can build in the rules or code, the data fields mentioned in **Section 3.1** above to extract the data.
- The auditor can provide this to the company's IT team to schedule the data extraction automatically.
- Once data is obtained, the auditor can also write scripts for the JE criteria to run automatically. The JE criteria is mentioned in Section 4.
- Based on the results obtained, the auditor can test the list of journal entries obtained after applying the filters.

Safeguards to be applied while using scripts:

- The auditor should be careful to see that the scripts are updated in all respects. For example – if the company has added a new period/ new journal type/new user id, the scripts should be updated immediately.
- The auditor should ensure that the company do not make any unauthorised changes to the script without the knowledge of the auditor. The scripts are the property of the auditor.
- The auditor should plan the process of extraction in such a way that the scripts are run by the company's IT team in the presence of the audit team and the output is provided to the auditor without any modifications.

7.6 Exercises

1. The unusual, non recurring transactions may generally be directly entered in

   (a) Sub ledgers

   (b) General Ledger

   (c) Excel sheets

   (d) None of the above

2. Estimates, impairments are generally a type of

   (a) Standard Journals

   (b) Top up journals

   (c) Non Standard journals

   (d) None of the above

3. While understanding the IT/ERP systems used to record entries, the points to note are:

   (a) Accounting software / ERP used

   (b) Automated or Manual entries

   (c) SA/SOD among IT and Business teams

   (d) Timing of passing the entries

   (e) All of the above

4. Some of the fraud risk factors to note which may lead to unusual transactions are:

   (a) Sales Targets

   (b) Personal gain such as Bonus, incentives etc.

   (c) Debts requirements for banks etc.

   (d) All of the above

5. A key factor to be kept in mind while making enquiries of personnel are:

   (a) Ask close ended questions

   (b) No discussions required

   (c) Ask open ended questions

   (d) None of the above

6. Entries maintained outside the system and impact the financial statements are:

   (a) Top up entries

   (b) Standard Journal entries

   (c) Non Standard Journal Entries

   (d) None of the above

7. Which is the main risk due to Non Standard Journal entries:

   (a) Risk of Material misstatement

   (b) Risk of management override of controls

   (c) Risk of lack of sensitive access

   (d) Risk of lack of segregation of duties.

8. It is possible that a Non standard journal entry may not have relevant _____________ supportings.

9. A common method to test for completeness of data is __________________ testing.

10. In industries/sectors, where volume of data is huge, _________________ testing may not be an appropriate way of testing completeness of data.

11. Before testing Journal entries, it is necessary to test the controls surrounding the process of passing Journal Entries.

    (a) True

    (b) False

12. One way of auditor enquiring about unusual activities at a client location is to ask ________ questions.

13. _______________ to be achieved may be a key fraud risk factor from an investor/ stock holder perspective leading to Non standard journal entries.

14. ______________ to be achieved may be a key fraud risk factor from a bank/financial institution perspective.

15. To bring in efficiencies in the process of extraction and analysis of JE data, the auditor may use ____________ .

7.7 References and further reading

1. Standards on Auditing published by the Institute of Chartered Accountants of India (ICAI), www.icai.org > Resources

2. Guidance Note on Audit of Internal Financial Controls Over Financial Reporting issued by Auditing and Assurance Standards Board. - (14-09-2015), www.icai.org

3. Companies Act 2013, www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf

7.8 Case Study

Access Ltd is an IT company with its headquarters in India and 6 branches across the globe - 2 in USA, 2 in Europe and 2 in Asia Pacific. The main revenue streams of the company are IT/ITES services. The company services customers in the Americas, Europe and Asia Pacific. They have 7 offices along with the Headquarters in India.

These 7 offices have their own administrative teams, finance teams , sales teams etc. They transact with the HQ as well amongst themselves. Each office is a Revenue centre and hence costs/expenses are tracked separately by them. The finance team individually draws up a TB, P&L account and B/S capturing their numbers separately. The books of accounts are maintained separately by each office and audited at the location by a locally appointed auditor. The signed audit report is sent to HQ for consolidation.

Since, the HQ is in India, the main auditors are located in India. The main auditors, audit the consolidated set of accounts.

The company is using SAP as their main ERP. Since, the company is a well established company with a large clientele, the number of transactions are substantial. Totally they have about 5000 transactions per month at the HQ. The transactions are passed by the Sales Personnel, Finance personnel etc. All the operations are automated and hence most of the entries automatically flow into the General Ledger. The Finance team as part of the book closure process also pass manual entries as appropriate.

You are a member of the audit team. You have been informed that the IT personnel in the team have evaluated and tested the GITC’s and found them effective. You have tested the Sensitive access (SA) and Segregation of Duties (SOD) as defined in the process and the system and found them effective. The other internal controls in the processes are also effective.

The audit strategy is to test Non standard Journal entries. You have been asked to devise a procedure to test the entries. You will discuss and finalise the audit procedure with your Audit Manager.

7.9 Answer to Exercise

1. Answer is b - General Ledger.

Generally, the non-recurring transactions may not have a supporting. To be passed in Sub ledgers, it may require collusion among personnel. Hence, they are passed in General Ledger.

2. Answer is c – Non Standard Journals.

   These are based on certain assumptions etc and not passed as part of a standard/routine operation.

3. The answer is e – All of the above.

   All the factors are necessary to be noted while understanding the IT/ERP system.

4. The answer is d – All of the above.

   All are relevant risk factors which may lead to unusual transactions.

5. The answer is c – Ask open ended questions

   By asking open ended questions, the auditor will be able to extract more information from the auditee. This will enable the auditor to ask more relevant questions.

6. The answer is a – Top up entries.

   These entries are usually passed after the books are closed and before the financial statements are finalised.

7. The answer is a – Risk of material misstatement.

   NSJE are entries that may be passed as a result of fraud. Hence, this is the main risk. Another risk can also be risk of management override of controls.

8. "Printed"

9. "Roll forward"

10. "Roll forward"

11. The answer is True.

    As part of the requirements of IFC, the controls pertaining to Journal entry process need also to be evaluated and tested.

12. "Open ended"

13. "Sales targets"

14. "Debt requirements"

15. "Software scripts"

7.10 ANSWER TO CASE STUDY

1. The HQ in India will have regular transactions and Inter company transactions.

2. As part of the evaluation of the IT and Business processes, the automated controls have been found to be effective. The journal types of automated entries should be identified.

3. Understand from the company, the manual entries and inter company entries passed. Understand the Journal type used for such entries.

4. Focus should be only on those entries. If the list of such entries can be separately extracted, the list should be reconciled with the TB and then tested.
5. If the separate list cannot be extracted:
   (a) the full list of entries should be extracted including automated entries.
   (b) Roll forward testing should be performed including the Opening and Closing Trial Balances
   (c) The automated transactions, based on the Journal types identified earlier should be removed from the list. Thus, only manual transactions remain.
   (d) From the manual transactions list, the inter company transactions should be removed.
   (e) On the remaining population, the auditor should apply the JE criteria and obtain a filtered list to test.
6. The full list of Intercompany transactions should be tested separately. A reconciliation statement may be sent to each office to confirm the balance.
7. The auditor may also speak to the component auditors to understand the procedures followed by them to test NSJE at the individual offices.

7.11 Glossary

NSJE - Non Standard Journal Entries

ERP – Enterprise Resource Planning

SA – Sensitive Access

SOD – Segregation of Duties

ACL – Automated Command Language

CAATS – Computer Assisted Audit Techniques