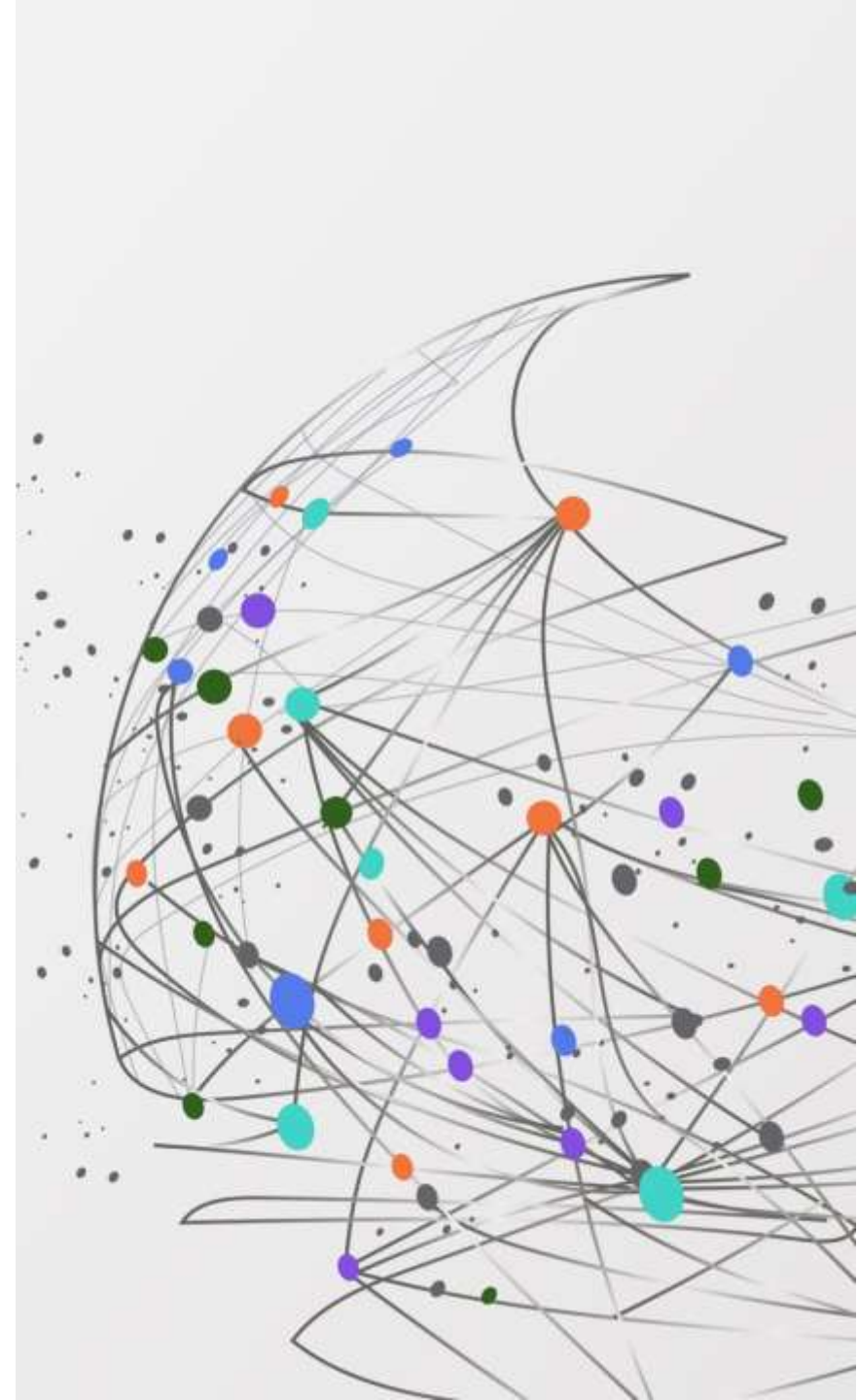


# Information Technology General Controls for Internal Financial Controls and Audit Trail

By

CA. S. Deephika B. Com, FCA, DISA



# Why should auditor equip on IT?

Increasing complexity of the IT setup

Trend of automation in business processes

Increased focus on effective operation of controls around IT assets and services.

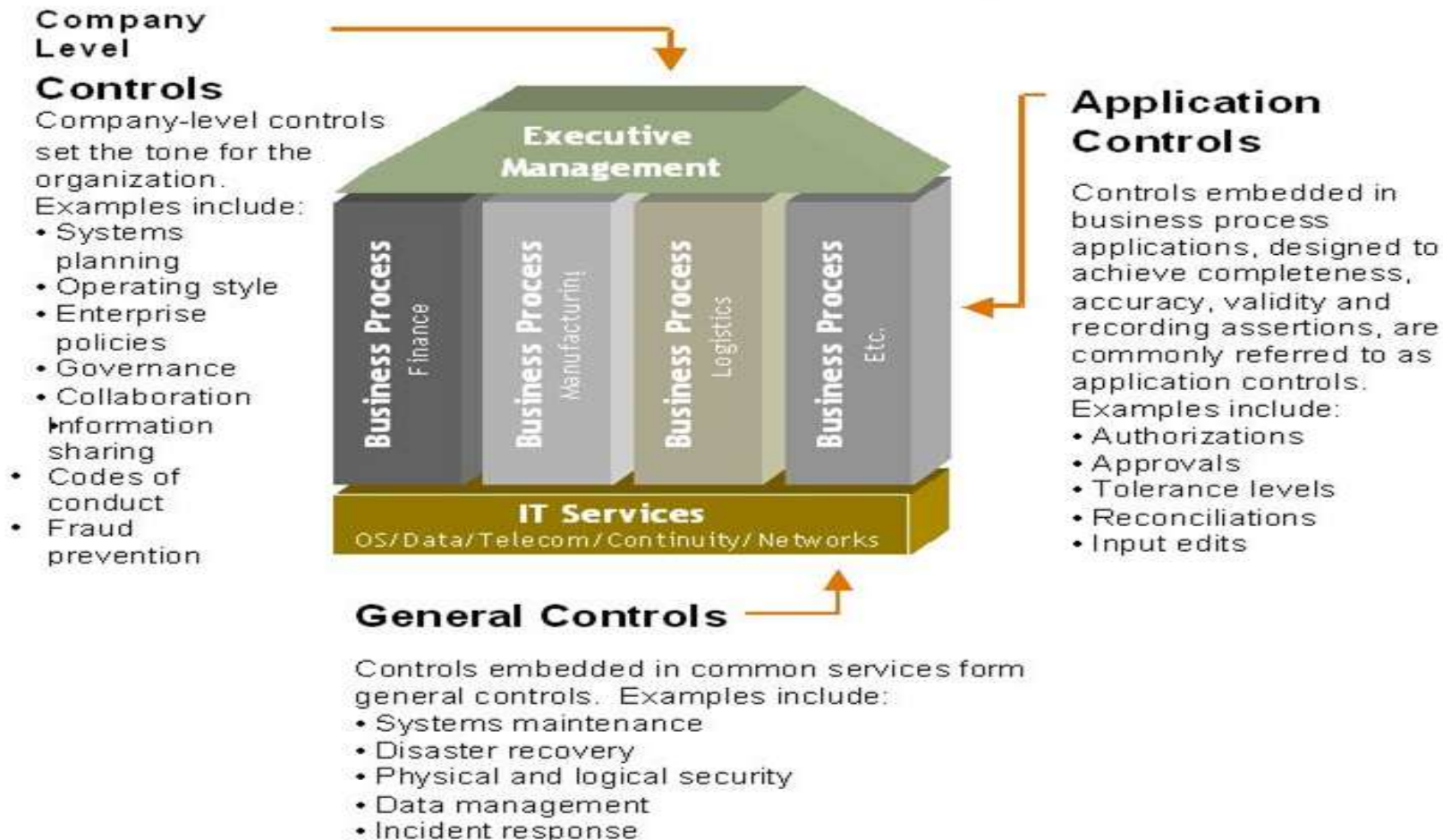
Multiple layers supporting IT infrastructure in the business process

Effect on Reporting in the financial statements

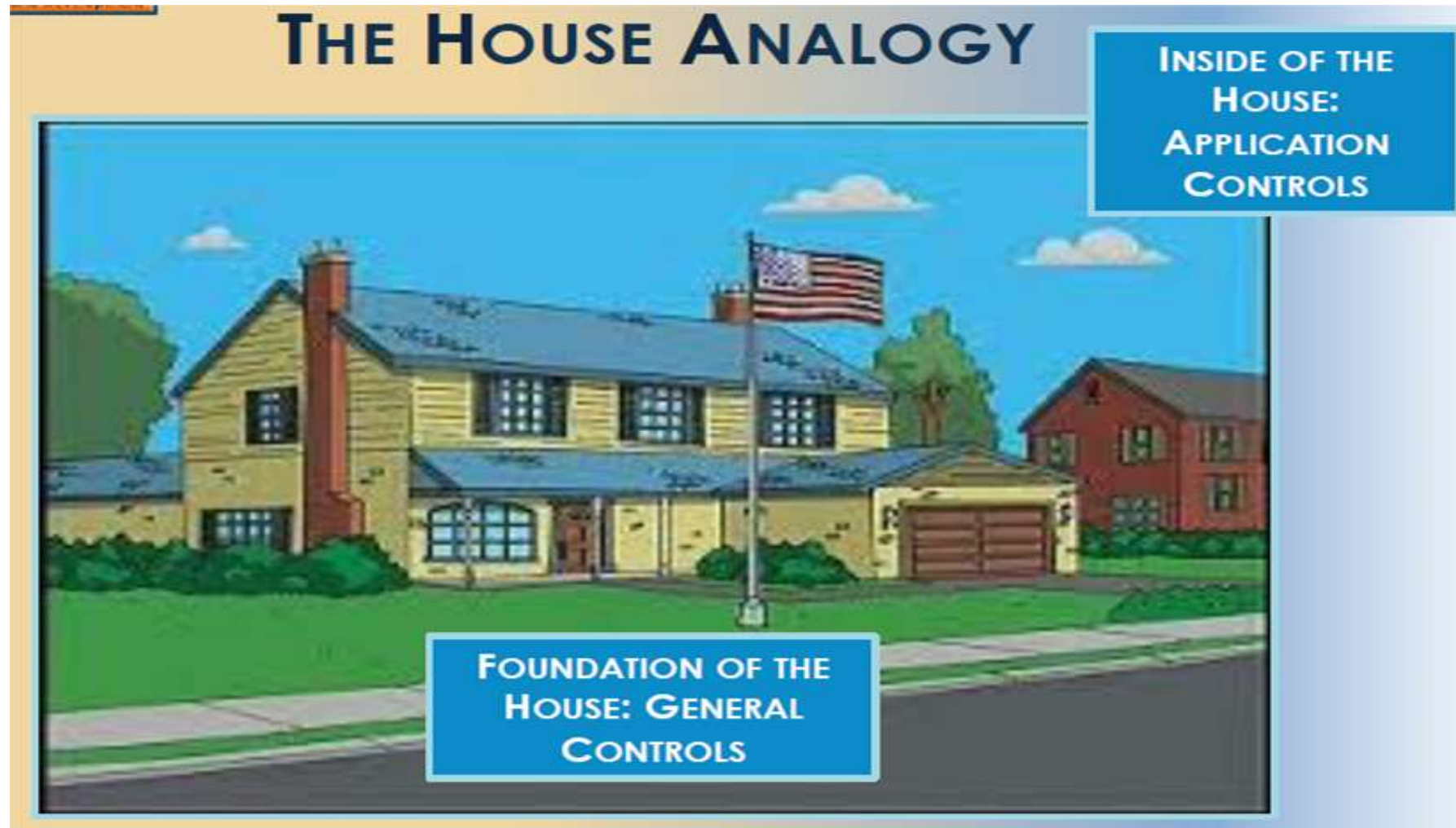
Impact on company's internal control over financial reporting.

Compliance with applicable laws and regulations (SA 315)

# Common elements of IT control



# IT General Controls Vs IT Application Controls



# Categories of Application Implementation

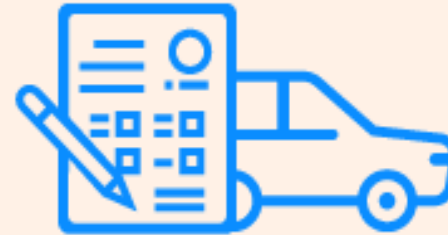
## YOUR OWN CAR

On-premises solution



## LEASED CAR

IaaS



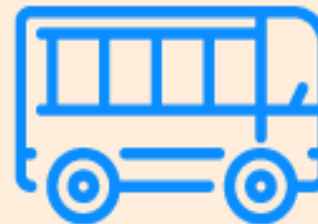
## TAXI

PaaS



## BUS

SaaS





## Shared Responsibility Model for Security in the Cloud

On-Premises (for reference)	IaaS (infrastructure-as-a-service)	PaaS (platform-as-a-service)	SaaS (software-as-a-service)
User Access	User Access	User Access	User Access
Data	Data	Data	Data
Applications	Applications	Applications	Applications
Operating System	Operating System	Operating System	Operating System
Network Traffic	Network Traffic	Network Traffic	Network Traffic
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

 Customer Responsibility

 Cloud Provider Responsibility

# Service organization certifications

Standards on auditing 402 - type 1 and type 2 reports

Service organization controls – type 1 and type 2

Statement on Standards for Attestation Engagements no. 16 (SSAE 16)

# IT General Controls - Overview

**IT General Controls (ITGC)** are policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems.

## Key Domains:

- IT Governance
- Physical and Logical access controls
- Information security and data privacy
- Change management and Incident management
- Asset Management - Hardware and Software
- Back ups
- Disaster Recovery Planning(DRP), Business Continuity Planning(BCP)



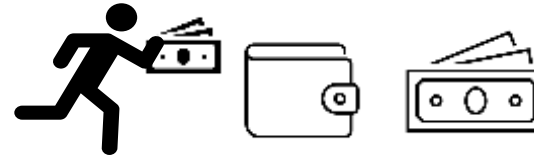
# 1. IT Governance

<b>IT Strategy</b>	Is a IT Operating Plan documented formally ? Is it broken into short term measurable plans ? How is the adherence to plan monitored ? Is there a IT Steering Committee ?
<b>IT Policies and Procedures</b>	Are Policies and Procedures documented and approved?
<b>IT Roles and Responsibilities</b>	Are roles and responsibilities for IT personnel (including Senior Management, Strategy Committee, Steering committee) well defined
<b>Data Ownership</b>	Is data ownership clear - IT and Business Owner responsibilities have been well defined ?
<b>IT Risk Assessments</b>	Are risk assessments of critical system performed ? If so, at what frequency ? How are risks identified addressed ?Is the risk register documented?

## 2. Physical and Logical access controls - Overview



**Protect staff and systems**



**Prevent intruders and theft**



**Audit trail and  
compliance with  
regulations**



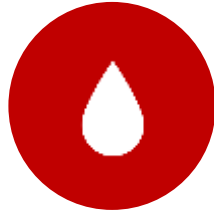
**Integration across  
physical and logical  
access**

## 2. Physical and Logical access controls – Contd...

### Physical access controls



**Fire**



**Water**



**Dust**



**Humidity**



**Perimeter**



**Doors**

## 2. Physical and Logical access controls – Contd...

### Logical access controls



User management



Session management



Suspension of  
inactive user ids



Privileged user access  
management



Password  
configuration

## 2. Physical and Logical access controls – Contd...

### LOGICAL ACCESS CONTROL - PRIVILEGED USER ACCESS M

User ID	User Name	Procurement							
		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

## 2. Physical and Logical access controls – Contd...

### LOGICAL ACCESS CONTROL – PASSWORD CONFIGURATION

The screenshot displays a software application with a navigation bar at the top containing tabs: Home, Procurement, Sales, Inventory, Quality, Engineering, Production, Master, and Import/Export. The 'Master' tab is selected.

On the left, the 'Party Details' section includes a 'Modify Search' button and a table of records. The table has columns for 'Party Code' and a selection column with radio buttons. The records listed are:

Party Code
C2CID21003
C2CID21002
C2CID21001
C2CID21000
C2CID20999
C2CID20998
C2CID20997
C2CID20915
C2CID20949
S30550333

Below the table, it says 'Time taken: 0.475 Sec.'

A 'Preferences' dialog box is open, showing tabs for 'Personalize Webtop', 'Organization Preferences', 'My Preferences', and 'Change Password'. The 'Change Password' tab is selected.

Within the 'Change Password' tab, a 'Password Policy' dialog box is displayed, listing the following rules:

- The password must have minimum of 1 and maximum of 15 lower case alphabets
- The password must have minimum of 1 and maximum of 15 upper case alphabets
- The password must have minimum of 2 and maximum of 15 Alphabets
- The password must have minimum of 1 and maximum of 15 Numeric Characters
- The password must have minimum of 1 Special Characters (#, ., !, @, \$, ~, .., -)
- The password must not contain the login id
- The password must not contain the first name
- The password must not contain the last name
- The password must not match last 3 passwords.
- The password must have a minimum length of 8 and a maximum length of 15.

The background interface also shows a 'Create' button and a table with columns 'Group' and 'Agent Code'. At the bottom right, the page number 'Page 1 of 121' is visible. The system tray at the bottom shows the date '04-10-2018' and time '11:08 AM'.



## 2. Physical and Logical access controls – Contd...

### LOGICAL ACCESS CONTROL – ENCRYPTION

sph_id	sph_log_id	sph_service_id	sph_username	sph_curr_password	sph_new_password	sph_status
2986	30	17164	onx6rebiYG6QTQ9lAr0ZJw==	F3n9TWEUv/nNtJOAqhF1...	hTrAajKXQ7lb+z4VG26Cf4J751H...	True
2987	31	17165	3ofg+4mk7huxb/pw8AmH4...	F3n9TWEUv/nNtJOAqhF1...	kIo8ynuzNAUIzR5NRxKzESAZxf...	True
2988	32	17166	onx6rebiYG6QTQ9lAr0ZJw==	F3n9TWEUv/nNtJOAqhF1...	rX1+5UFJnxg/YrLyFpyxxg==	True
2989	33	17167	3ofg+4mk7huxb/pw8AmH4...	F3n9TWEUv/nNtJOAqhF1...	WO0KC9+qFRkVLTpx8mLCyWaK...	True
2990	34	17167	3ofg+4mk7huxb/pw8AmH4...	F3n9TWEUv/nNtJOAqhF1...	o4QR8HasgIgfERutlDmjZ6WL3vJ...	True
2991	35	17168	9NdUZWI3j+jSFZe+TQCRLg...	F3n9TWEUv/nNtJOAqhF1...	o4QR8HasgIgfERutlDmjZ6WL3vJ...	True
2992	36	17169	3ofg+4mk7huxb/pw8AmH4...	F3n9TWEUv/nNtJOAqhF1...	VrUvwk+QyuNPGozHQ8JLEhb32...	True
2993	37	17169	3ofg+4mk7huxb/pw8AmH4...	F3n9TWEUv/nNtJOAqhF1...	lOQqI0iLoczZdL86iV505FXwHo1...	True
2994	38	17170	3ofg+4mk7huxb/pw8AmH4...	F3n9TWEUv/nNtJOAqhF1...	jz5JJWcmn8sq23KWhLS7Cx5VE...	True
2995	39	17171	3ofg+4mk7huxb/pw8AmH4...	F3n9TWEUv/nNtJOAqhF1...	o4QR8HasgIgfERutlDmjZ6WL3vJ...	True

User ID	Password	Password hash value
ORACLE	ORACLE	38E38619A12E0257
ORADBA	ORADBAPASS	C37E732953A8ABDB
DBSNMP	DBSNMP	E066D214D5421CCC
DEMO	DEMO	4646116A123897CF
ADMIN	JETSPEED	CAC22318F162D597

## Questions and Answers

1. The type of access that auditors request should be \_\_\_\_\_

- A. Display-only
- B. Read-only
- C. Either A or B
- D. Both A and B

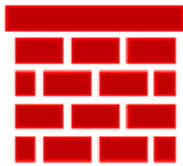
2. General IT controls are known as \_\_\_\_\_ controls

- A. Pervasive
- B. Indirect
- C. Both A & B
- D. None of the above

### 3. Information Security



Network security



Firewall



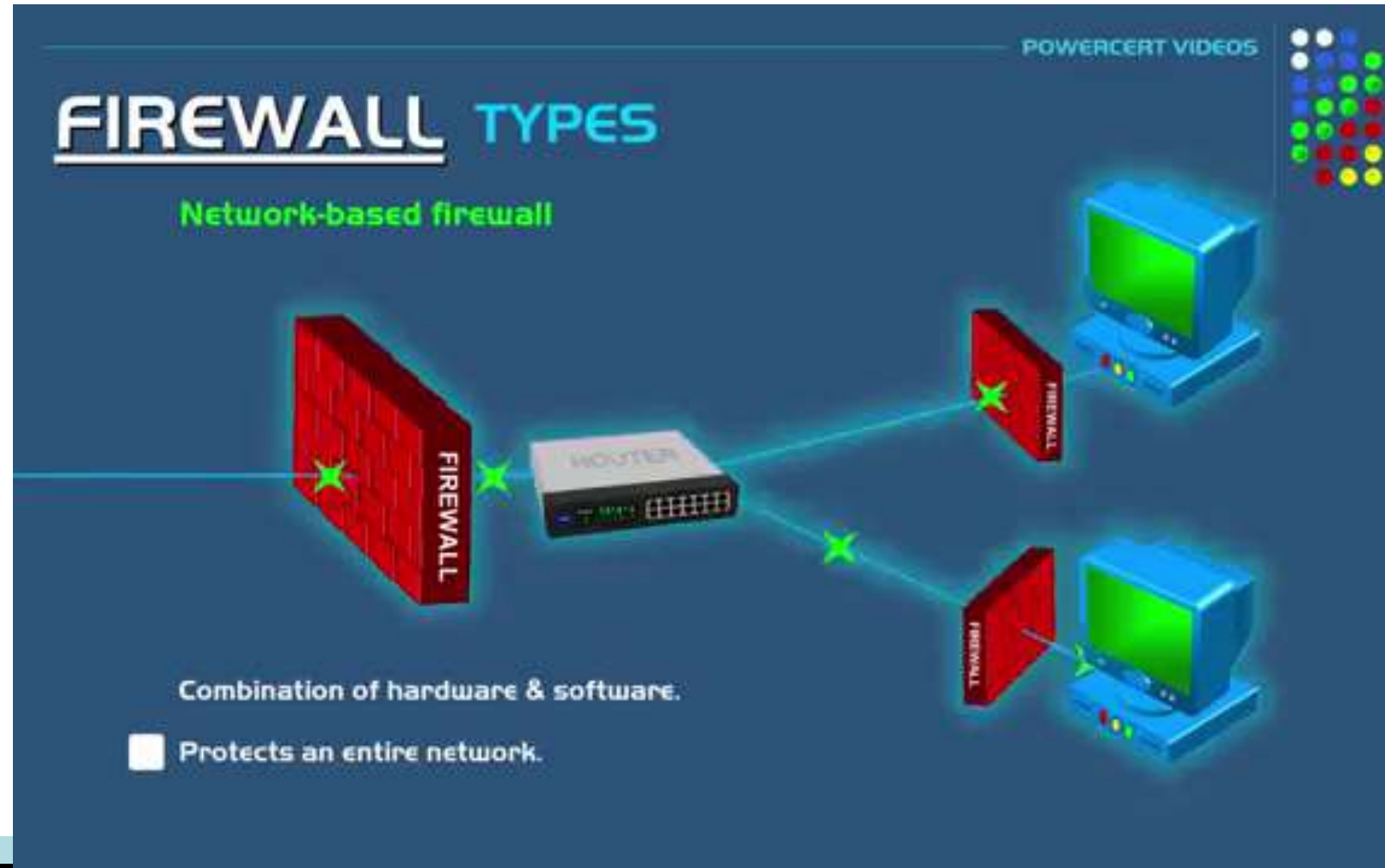
System Performance Management



Antivirus

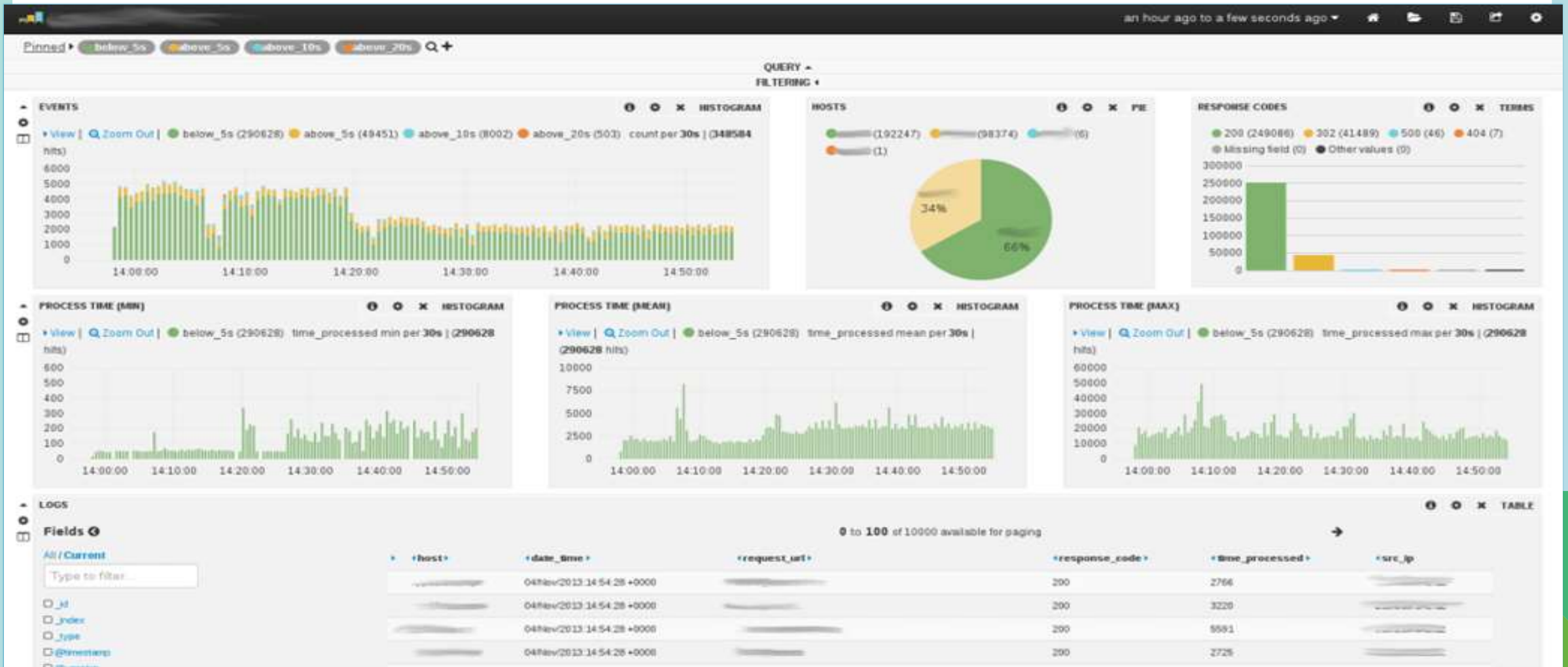
### 3. Information Security – Contd...

#### FIREWALL

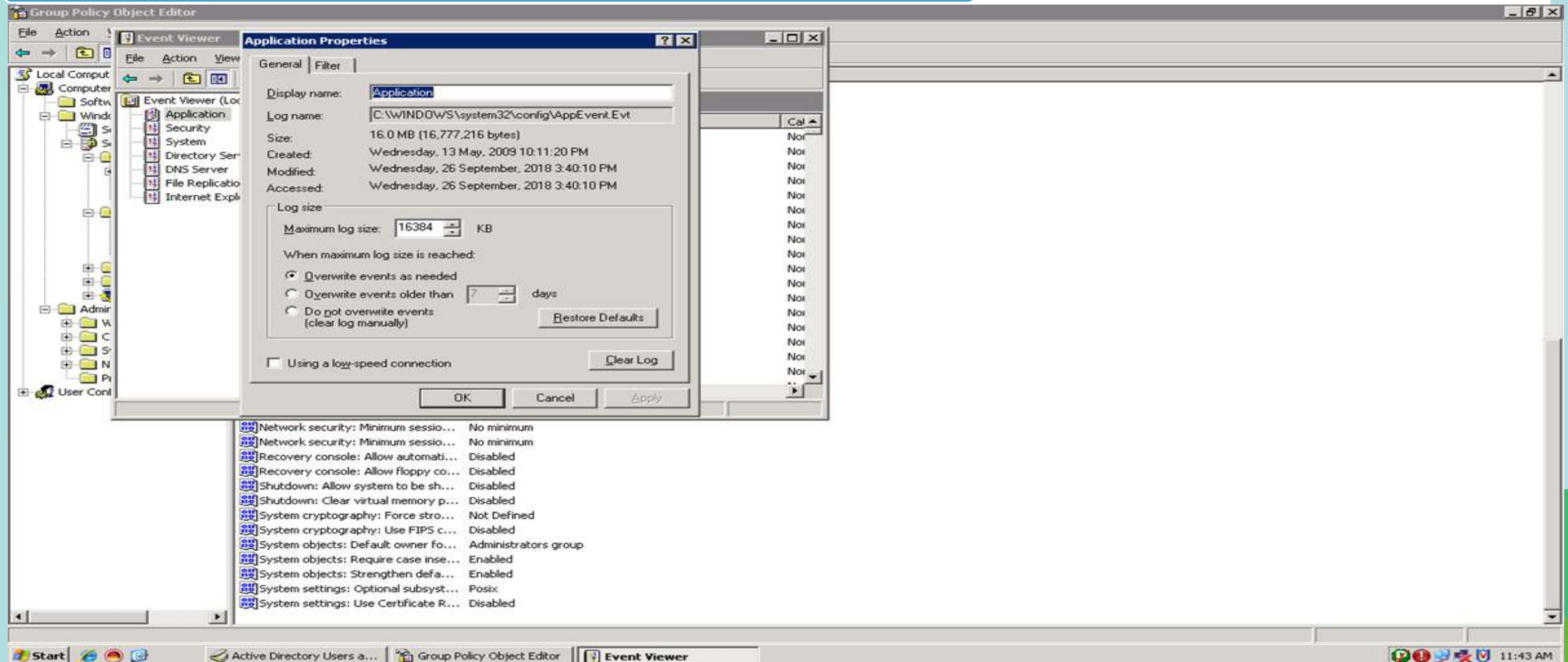


# 3. Information Security – Contd...

## SERVER PERFORMANCE

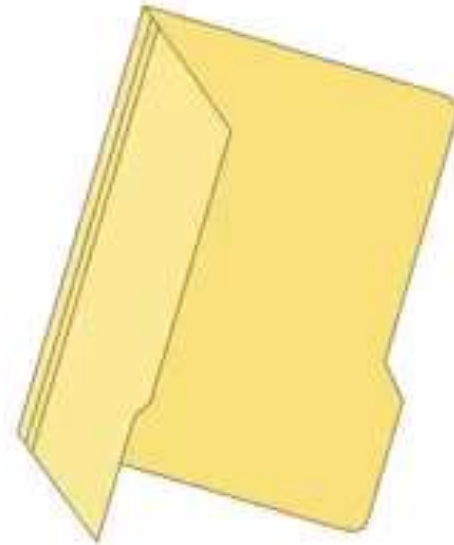


### 3. Information Security – Contd...



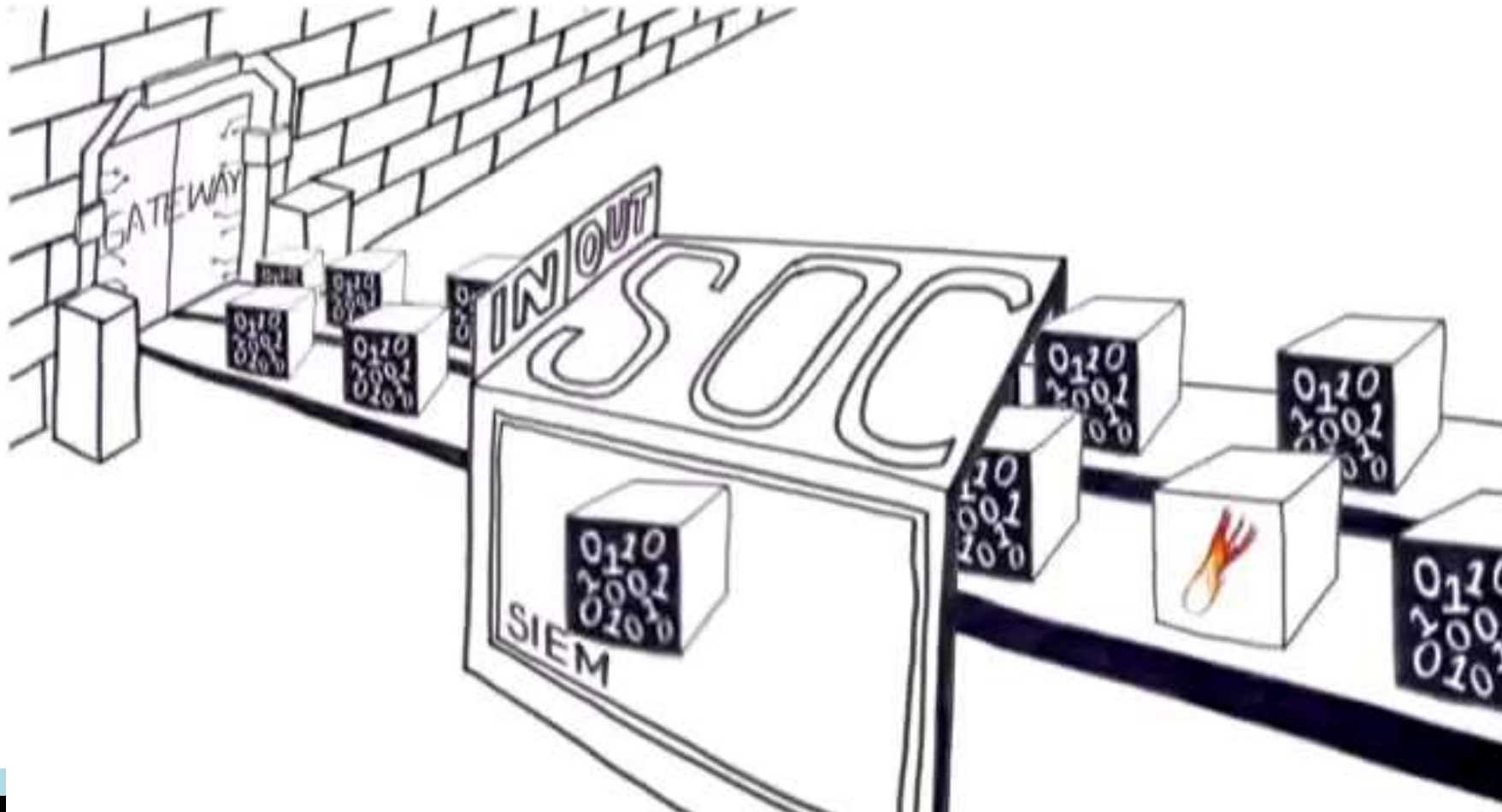


### 3. Information Security – Contd...



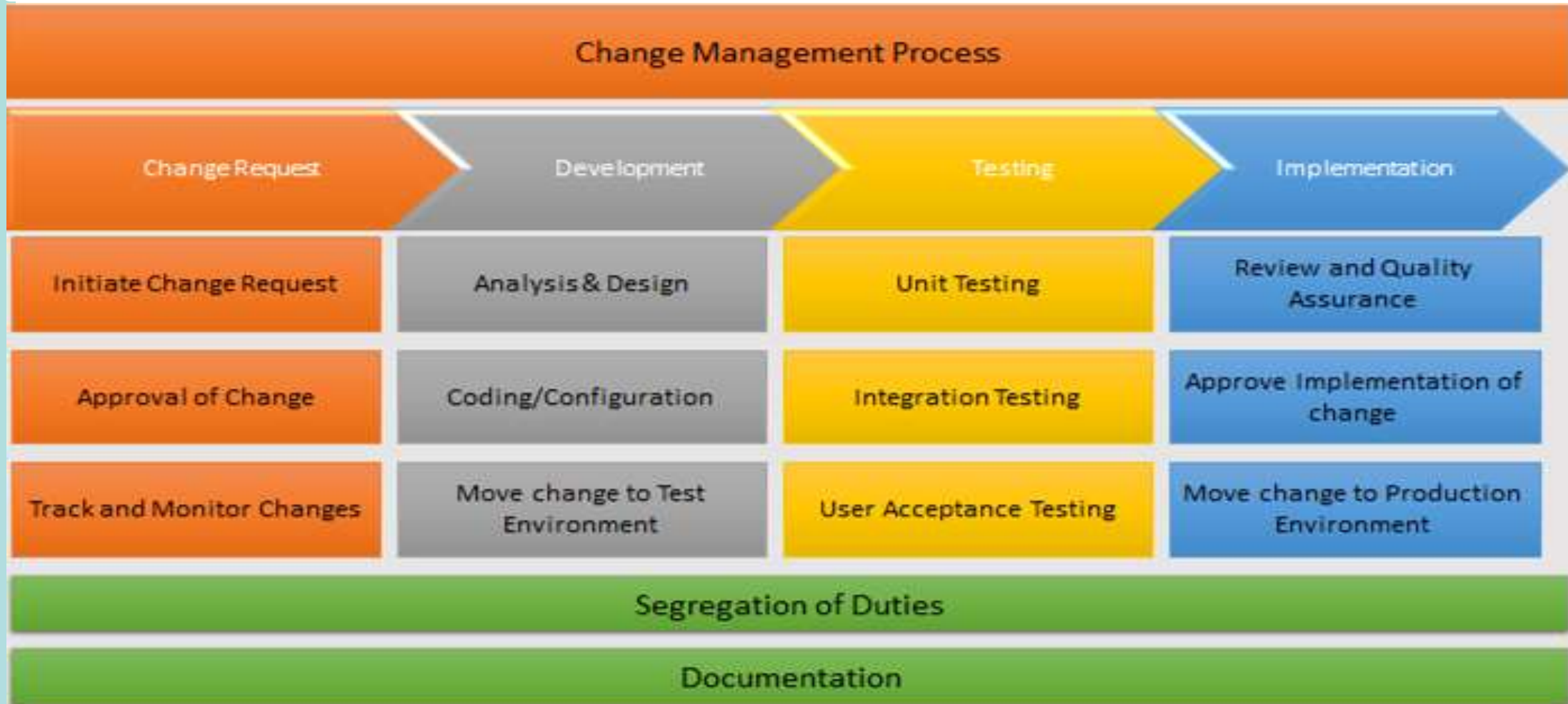
### 3. Information Security – Contd...

SOC



## 4. Change management and Incident management – Contd...

### CHANGE MANAGEMENT PROCESS



## 4. Change management and Incident management – Contd...

### CHANGE MANAGEMENT PROCESS – CHANGE REQUEST

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)

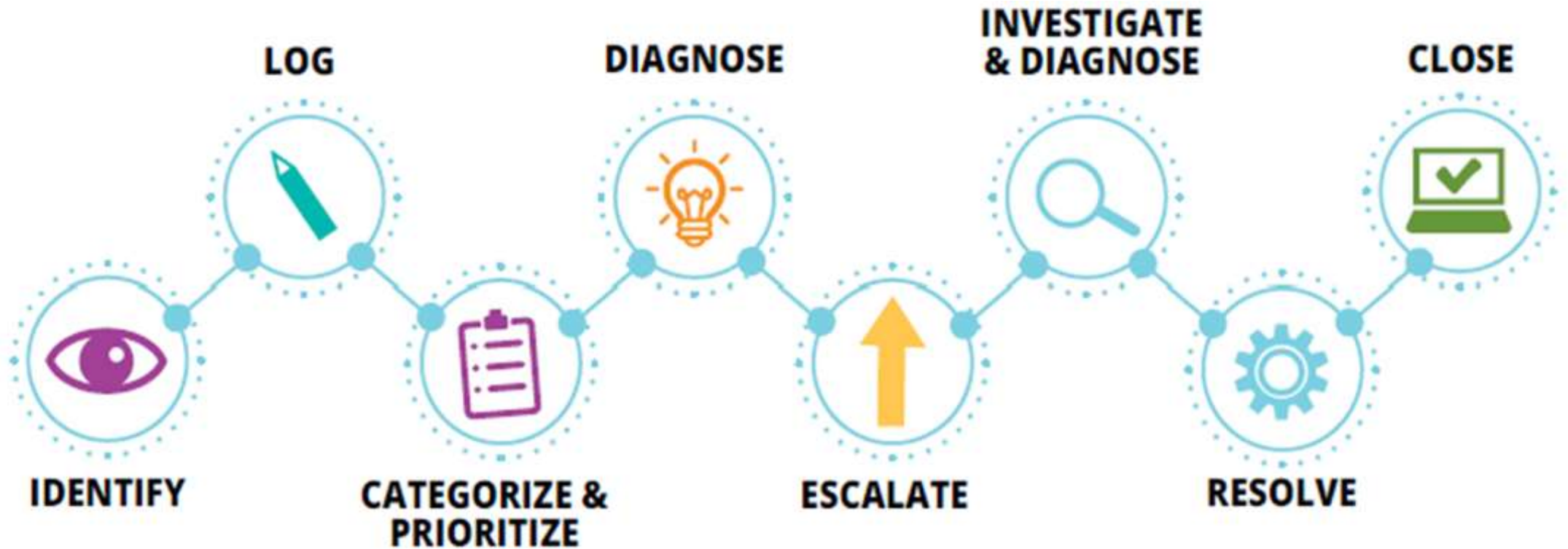
**Developed by**  
(Sign, Name & Date)

**Change Implemented by**  
(Sign, Name & Date)

**IT In-Charge / IT Head**  
(Sign, Name & Date)

## 4. Change management and Incident management – Contd...

### INCIDENT MANAGEMENT





## 5. Asset Management - Hardware and Software

### HARDWARE ASSET MANAGEMENT

Asset Lifecycle





## 5. Backups - Review



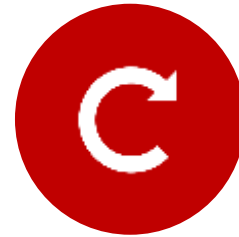
**Content**



**Frequency**



**Storage**



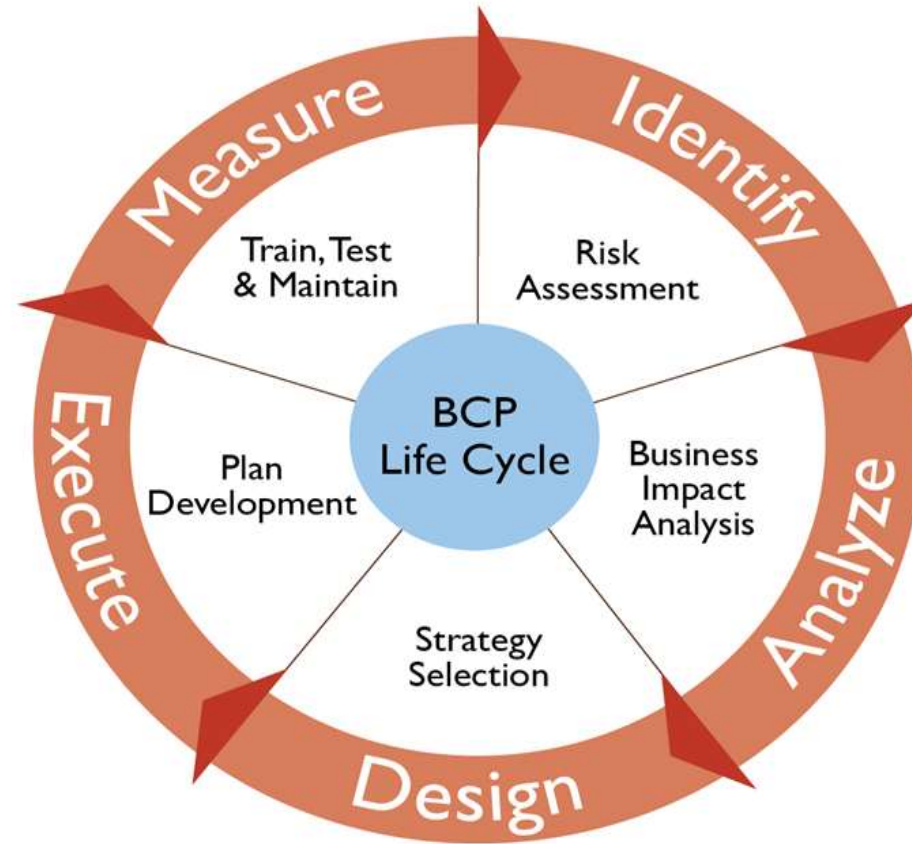
**Restore**



**Restricted access**

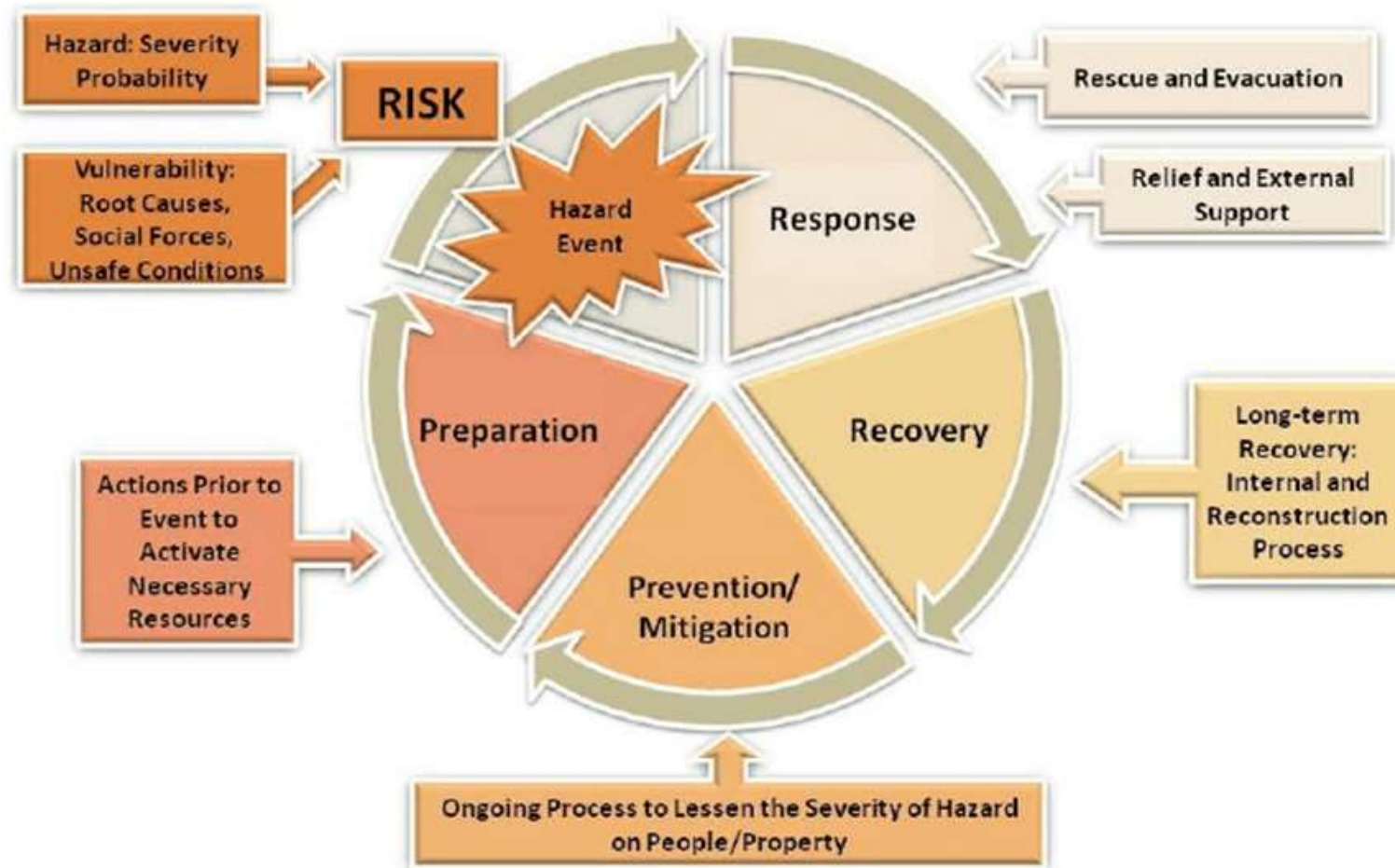
## 6. DRP and BCP – Contd...

### BCP LIFE CYCLE




## 6. DRP and BCP – Contd...


### DRP LIFE CYCLE



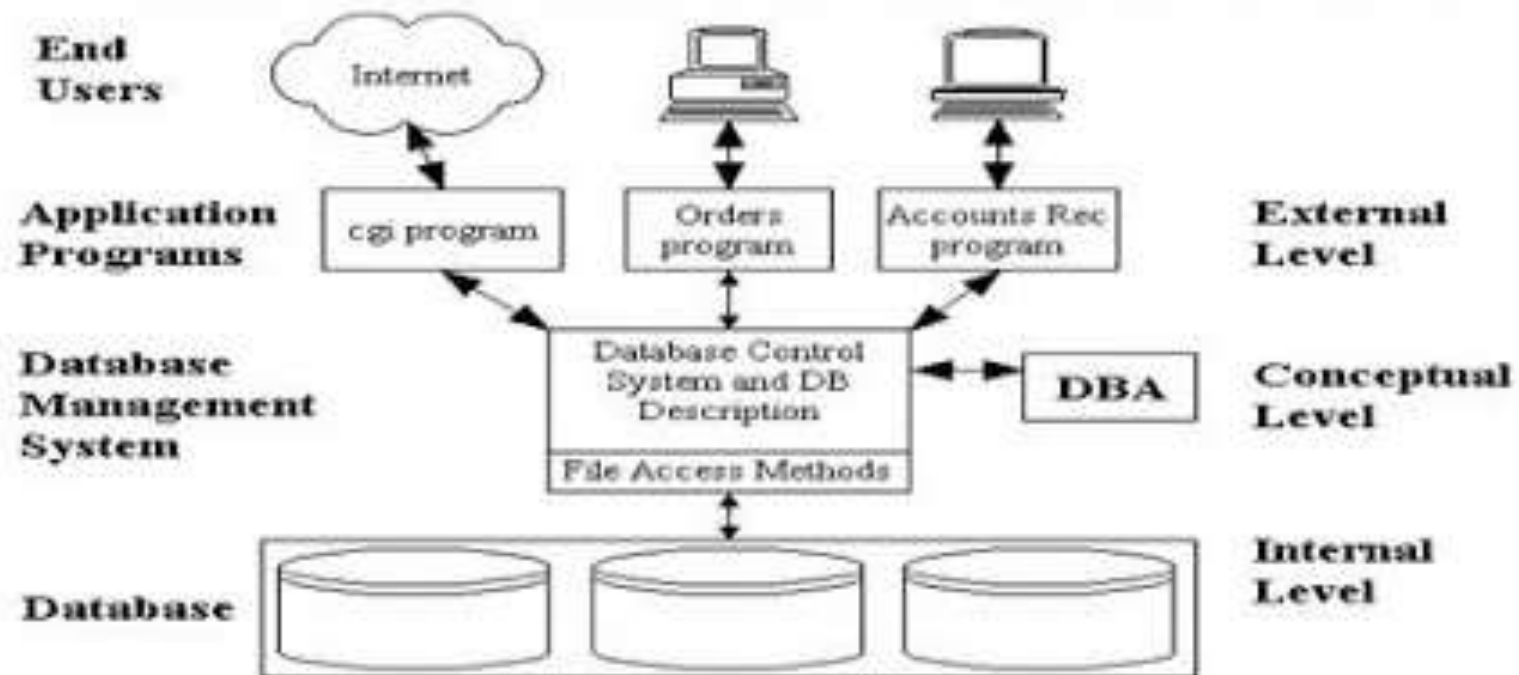
## Questions and Answers

3. The reliability of an application system's audit trail may be questionable if:
- A. user IDs are recorded in the audit trail.
  - B. the security administrator has read-only rights to the audit file.
  - C. date and time stamps are recorded when an action occurs.
  - D. users can amend audit trail records when correcting system errors.
- 
- A decorative graphic in the bottom right corner consisting of several overlapping green triangles and squares of varying shades, creating a modern, abstract design.

## Work from Home Risks

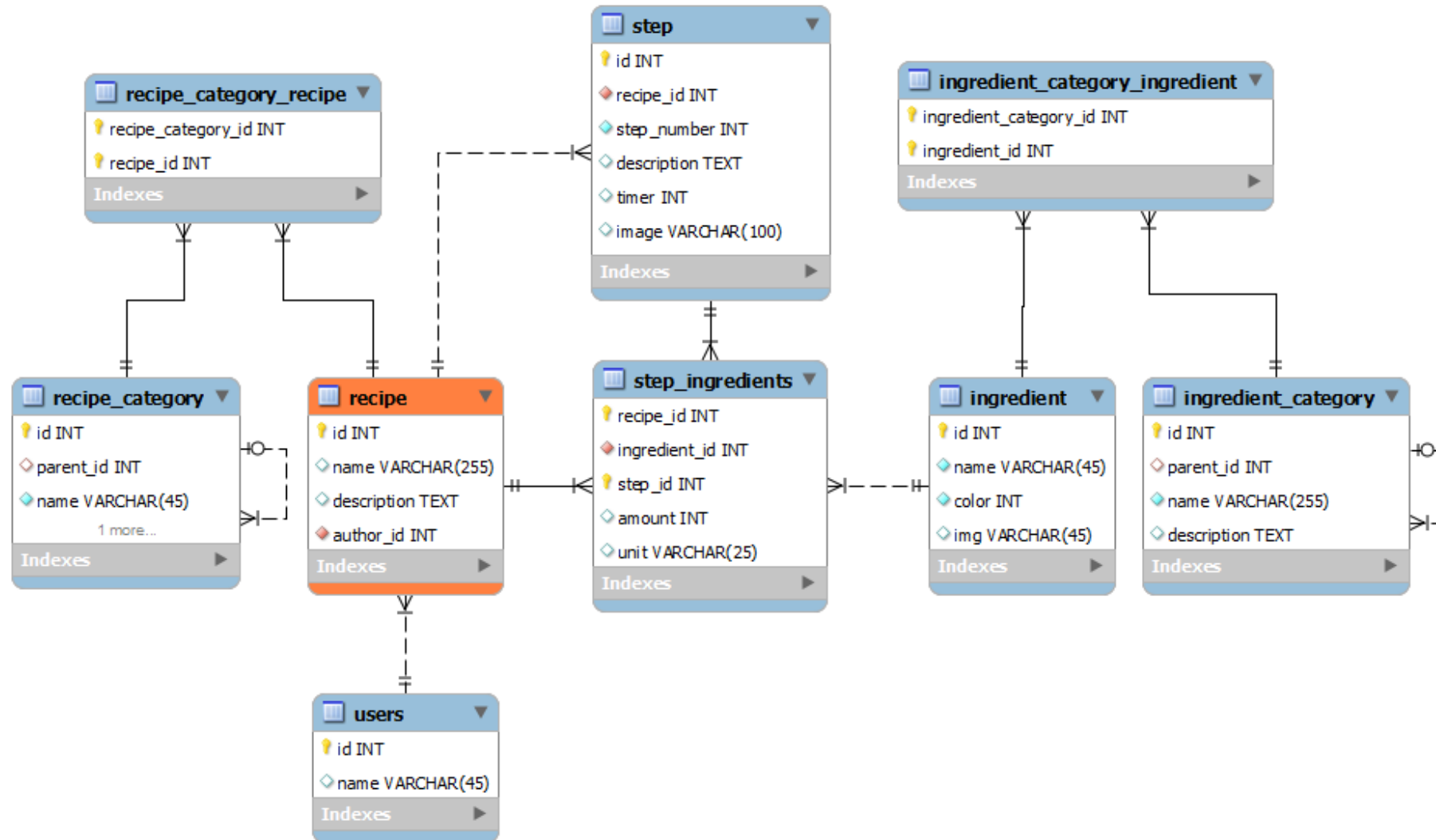
- ⌘ Social Engineering
  - ⌘ Shoulder browsing
  - ⌘ Data loss/ Data theft
  - ⌘ Device security/ BYOD
  - ⌘ Patch Management.
  - ⌘ Employee training
- 
- A decorative graphic in the bottom right corner consisting of several overlapping green triangles and squares in various shades of green.

# Database Architecture





# Database Table Architecture



# Database Table Console

Home > Databases and Clusters > VMart > Query Runner

Query History

Clear all

Filter previous queries

SELECT sales\_quantity,  
sales\_dollar\_amount,  
transaction\_type, cc\_name FROM  
online\_sales.online\_

SELECT sales\_quantity,  
sales\_dollar\_amount,  
transaction\_type, cc\_name FROM  
online\_sales.online\_

SELECT sales\_quantity,  
sales\_dollar\_amount,  
transaction\_type, cc\_name FROM  
online\_sales.online\_

SELECT sales\_quantity,  
sales\_dollar\_amount,  
transaction\_type, cc\_name FROM  
online\_sales.online\_

SELECT sales\_quantity,  
sales\_dollar\_amount,  
transaction\_type, cc\_name FROM  
online\_sales.online\_

1 SELECT sales\_quantity, sales\_dollar\_amount, transaction\_type, cc\_name  
2 FROM online\_sales.online\_sales\_fact  
3 INNER JOIN online\_sales.call\_center\_dimension  
4 ON (online\_sales.online\_sales\_fact.call\_center\_key  
5 = online\_sales.call\_center\_dimension.call\_center\_key  
6 AND sale\_date\_key = 156)  
7 ORDER BY sales\_dollar\_amount DESC;  
8 SELECT order\_number, date\_ordered  
9 FROM store.store\_orders\_fact orders  
10 WHERE orders.store\_key IN (  
11 SELECT store\_key  
12 FROM store.store\_dimension  
13 WHERE store\_state = 'MA')  
14 AND orders.vendor\_key NOT IN (  
15 SELECT vendor\_key  
16 FROM public.vendor\_dimension  
17 WHERE vendor\_state = 'MA')  
18 AND date\_ordered < '2012-03-01';  
19 SELECT store\_key, order\_number, date\_ordered

Execute Queries

SELECT sales\_quSELECT order\_nuSELECT store\_ke

Query ResultsQuery PlanQuery ProfileExport DataAuto-Resize all columnsSearch query results

sales_quantity	sales_dollar_amount	transaction_type	cc_name
7	589	purchase	Central Midwest
8	589	purchase	South Midwest
8	589	purchase	California

2514 rows | Execution time: 0.113s

Overview

Activity

Manage

Design

Load

Query Execution

Query Plan

License

Settings



## Vulnerabilities in Database

Excessive  
access  
privileges

Data  
Isolation

Un-encryption



# Maintenance of Audit Trail

**Extract from the MCA Notification dated 24<sup>th</sup> March, 2021 (new proviso inserted in Rule 3 – sub rule (1) of Companies (Accounts) Rules 2014:**

“Provided that for the Financial Year commencing on or after the ~~1<sup>st</sup> day of April, 2021~~\* Every company which uses **accounting software** for maintaining its books of account, shall use only such accounting software which has a feature of **recording audit trail for each and every transaction, creating an edit log** of each change made in the books of account along with the date when such changes were made and ensuring that the audit trail cannot be disabled.”

“Whether the company has used such accounting feature for maintaining its books of account which has a feature of recording audit trail (edit log) facility and the same has been operated **throughout the year for all transactions recorded** in the software and the audit trail feature has **not been tampered** with and the audit trail has been preserved by the company as per the statutory requirements for record retention.”

\*Date was deferred to 1<sup>st</sup> April 2022, and then to 1<sup>st</sup> April, 2023

## Key Definitions

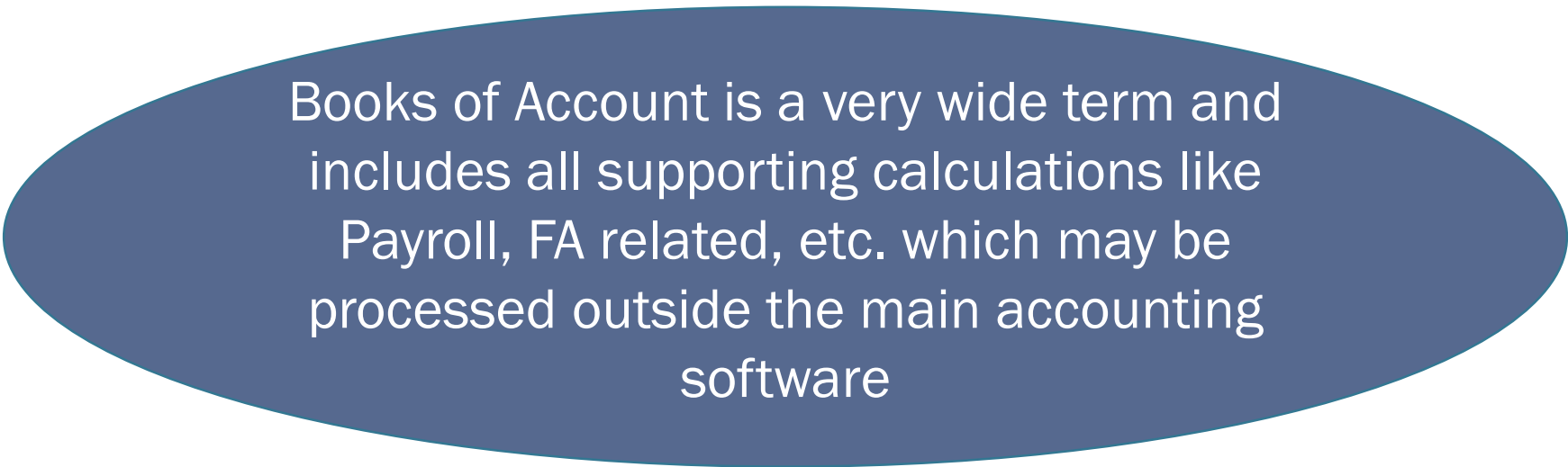
**"Books of Account" as per Section 2(13) of the Act includes records maintained in respect of**

- (i) all sums of money received and expended by a company and matters in relation to which the receipts and expenditure take place;**
- (ii) all sales and purchases of goods and services by the company;**
- (iii) the assets and liabilities of the company; and**
- (iv) the items of cost as may be prescribed under section 148 in the case of a company which belong**

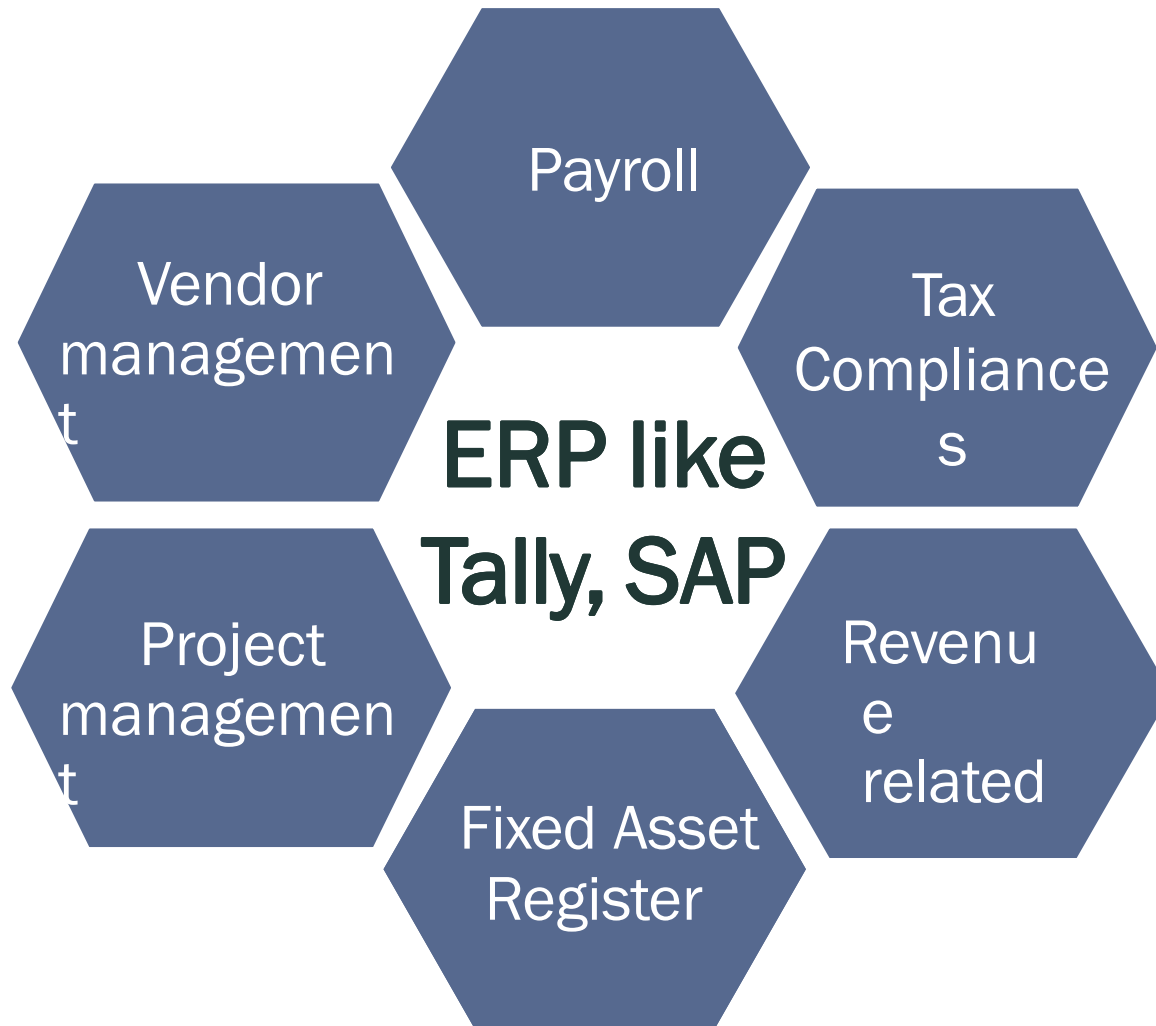
## Key Definitions

**“Accounting Software” is a computer program or system that enables recording, maintenance and reporting of books of account and relevant ecosystem applicable to business requirements.**

(Includes On-premise or on-cloud or subscribed to as Software as a Service (SaaS) software or a company may be using software which is maintained at a service organization. )



Books of Account is a very wide term and includes all supporting calculations like Payroll, FA related, etc. which may be processed outside the main accounting software



Books of Accounts can be in Multiple Software

...could be hosted in India or outside India or maybe on-premise or on Cloud of subscribed as SaaS

... or maintained at a service organization

... or even in Works Sheets



## Key Definitions

As per the Companies (Registration of Foreign Companies) Rules, 2014, the provisions of “Chapter X of the Act: Audit and Auditors” and Rules made there under apply, mutatis mutandis, **to a foreign company** as defined in the Act. Accordingly, the above reporting requirements would be applicable to the auditors of foreign companies as well.

Audit Trail applicable on both in case of **standalone financial statements and consolidated financial statements.**

It is not applicable to other entities like LLP, Partnership Firm, Sole prop etc.

# Maintenance of Back-ups

- **Maintaining of backups:** Rule 3(5) of the Accounts Rules requires every company to maintain **proper system for storage, retrieval**, display or printout of the electronic records as the Audit Committee, if any, or the Board of Directors may deem appropriate and such records should not be disposed of or rendered unusable, unless permitted by law. Additionally, companies are required to maintain the back-up of the books of account and other relevant books and papers in an electronic mode on servers **physically located in India on a daily basis (earlier periodic basis)** even in cases where such backups are maintained at a place outside India.
- **Effective date:** The amended Rules are effective from 11 August 202

# Maintenance of Back-Ups

**Service provider:** Rule 3(6) of the Accounts Rules requires disclosure by a company to the Registrar of Companies (ROC) in case a service provider has been used for maintenance of books of accounts in an electronic form. The amendments require an additional disclosure relating to the name and address of the person in control of the books of account and other books and papers in India, where the service provider is located outside India.

The revised requirements to be disclosed to the ROC on an annual basis at the time of filing of financial statement are:

- The name of the service provider
  - The internet protocol(IP) address of service provider
  - The location of the service provider (wherever applicable)
  - Where the books of account and other books and papers are maintained on a cloud, such address as provided by the service provider
  - Details of where the service provider is located outside India, the name and address of the person in control of the books of account and other books and papers in India.
- 
- Effective date: The amended Rules are effective from 11 August 2022.

# Statutory auditor responsibility

Auditor to comment on whether the company is using an accounting software which has a feature of recording audit trail, the auditor is expected to verify the following aspects:

- whether the audit trail feature is configurable (i.e., if it can be disabled or tampered with)?
- whether the audit trail feature was enabled/operated throughout the year?
- whether all transactions recorded in the software are covered in the audit trail feature?
- whether the audit trail has been preserved as per statutory requirements for record retention?

## Applicability

- Audit reporting triggered for FY commencing on or after 1<sup>st</sup> April 2022
- Applicability of Companies (Accounts) Rules commences on or after 1<sup>st</sup> April 2023
- In absence of compliance requirement by Companies, auditors cannot report for FY 2022-23
- Illustrative reporting for this can be as under:
  - *As proviso to Rule 3(1) of the Companies (Accounts) Rules, 2014 is applicable only w.e.f. 1<sup>st</sup> April 2023, reporting under this clause is not applicable”*
- Reporting applies both to SFS and CFS
  - Reporting for CFS would be based on the reporting done by Component Auditors
  - Would not be applicable to entities of the group not registered in India under Companies Act, 2013 (like foreign entities, LLPs, etc.)

- Management has a responsibility for effective implementation of the requirements prescribed by account rules
- Thus, it is the management, who is primarily responsible for ensuring selection of the appropriate accounting software for ensuring compliance with applicable laws and regulations (including those related to retention of audit logs).
- The Companies (Accounts) Rules 2014 states that accounting software should be capable of creating an edit log of "each change made in the books of account"
- Auditors' responsibility has been prescribed for "all transactions recorded in the software" –responsibility is restricted to transactions that have been recorded in the software and subsequent changes thereto –  
There is no responsibility for transactions NOT RECORDED in the software.

## Audit Approach

The auditor would need to ensure that the management assumes the primary responsibility to

- Identify the records and transactions that constitute books of account under section 2(13) of the Act;
- Identify the software i.e., IT environment including *applications, web-portals, databases, Interfaces, Datawarehouse, data lakes, cloud infrastructure, or any other IT component used for processing and or storing data for creation and maintenance of books of account;*