The Institute of Chartered Accountants of India

SIA – 520 and 530

Date : 27th May 2023

Speaker: CA Rekha Surana

Table of Contents

1. Overview of Standards on Internal Audit

The Internal Audit Standards are classified into various series for ease of identification and grouping of similar topics:-

- 100 Series: Standards on Key Concepts
- 200 Series: Standards on Internal Audit Management
- 300–400 Series: Standards on the Conduct of Audit Assignments
- 500 Series: Standards on Specialized Areas
- 600 Series : Standards on Quality Control
- 700 Series : Other/Miscellaneous Matters

Note: SIA 5 (Sampling), SIA 6 (Analytical Procedures), SIA 7 (Quality Assurance in Internal Audit), SIA 11 (Consideration of Fraud in an Internal Audit), SIA 18 (Related Parties) were issued up to July 1, 2013

1. Overview of Standards on Internal Audit (Contd).

Standard on	SIA	SIA Name
Key Concept (100 Series)	110	Nature of Assurance
	120	Internal Controls
	130	Risk Management
	140	Governance
	150	Compliance with Laws and Regulations
Internal Audit Management (200 Series)	210	Managing the Internal Audit Function
	220	Conducting Overall Internal Audit Planning
	230	Objectives of Internal Audit
	240	Using the Work of an Expert
	250	Communication with those charged with Governance
Conduct of Audit Assignments (300 Series)	310	Planning the Internal Audit Assignment
	320	Internal Audit Evidence
	330	Internal Audit Documentation
	350	Review and Supervision of Audit Assignments
	360	Communication with Management
	370	Reporting Results
	390	Monitoring and Reporting of Prior Audit Issues
Specialized Areas (500 Series)	520	Internal Auditing in an Information Technology Environment
	530	Third Party Service Provider

2a. Objectives of SIA 520

The overall objectives of an internal audit **do not change in an ITE**. However, the different nature of risks, and the controls required to mitigate those risks, do impact the audit approach and procedures deployed in the ITE. An audit in an ITE aims to evaluate an organization's IT risks and establish whether IT related controls are adequate to achieve organization's business objectives.

Audits are undertaken after due **study and understanding of the Organisation's ITE** covering:

a) IT Strategy

b) IT Policies

c) Operating Procedures

d) Risks and governance mechanism

An independent risk assessment, along with an **evaluation of the controls** required to mitigate those risks, forms the basis of the audit procedures

Audit procedures are sufficient to allow an independent assurance. Example:

a) Security and reliability of information

b) Efficiency and effectiveness of information processing

c) Analysis and reporting of the information

d) Continuous access and availability of the information

e) Compliance of the IT related laws and regulations

The overall objective of performing an internal audit in an ITE is to provide independent assurance and help in making improvements in the ITE, thereby enabling the **achievement of business objectives**

2b. Requirements of the Standard

1. IT Understanding and Risk Assessment

- Understanding the IT Landscape-IT Applications used for various business Processes, Infrastructure, Interfaces, IT Organization Structure, Strategy, Policies and Procedure, IT Risk assessment (Refer "Illustrative IT Landscape").

2. Internal Auditor Credentials

- IT audit qualification, Knowledge about ERP, and other emerging technologies.

3. IT Audit Scoping

- Auditor to identify the scope of IT Audit procedures Eg: IT Strategy, Governance and Oversight Audit , IT General Controls (ITGC) Testing, Automated Business Controls, System Reports Testing, IT Operations Audit, Cyber Security Audit, Emerging Audit Tools and Technologies, Compliance and Regulatory Requirement and Disaster Recovery and Business Continuity.

4. IT Audit Planning

An Internal Audit Assignment plan including the IT audit approach, methodology and timelines will be defined, documented and maintained, based on the objectives and audit scope identified above.

2b. Requirements of the Standard (Contd.)

5. Audit Execution

Performing interviews, review of supporting documentation, review of system configuration, inspection, and physical walkthrough. Understanding and scoping, IT risk assessment, IT Audit planning, IT risk and controls matrix, IT test work papers, system generated reports with the supporting documents, evidences gathered and so on. additional evidence or information, such as, risk mitigating measures provided by auditee to be considered before concluding on a test of IT controls

6. Audit Documentation

Professional Skill, care , due diligence to be applied. documentation shall include IT environment Internal Auditing in an Information Technology Environment

7. Management Discussion on Deficiencies

Final Deficiency and the corrective action and timeline to be discussed with management

2c. Key Terminologies

Database

An organized collection of structured information, or data, typically stored electronically in a computer system

Application

A comprehensive, self-contained program that performs a particular function directly for the user.

Server

A computer program or device that provides a service to another computer program and its user, also known as the client.

Firewall

A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Router

A networking device that forwards data packets between computer networks

Data Centre

A facility that centralizes an organization’s shared IT operations and equipment for the purposes of storing, processing, and disseminating data and applications.

Network Diagram

A visual representation of a components that make up a network and how they interact in a computer or telecommunications network.

2c. Illustrative IT Application Landscape – Manufacturing Company

Applications used:

App 1 (Financial Accounting) –Home grown Application –Sever in house
App 2 (Indirect Mat, FA, Payroll)-Licensed Application-Server on cloud
App 3 (FA)-Homegrown Application Server inhouse
App 4 (Attendance Recording)-SaaS based application , Server in-house

Legends used

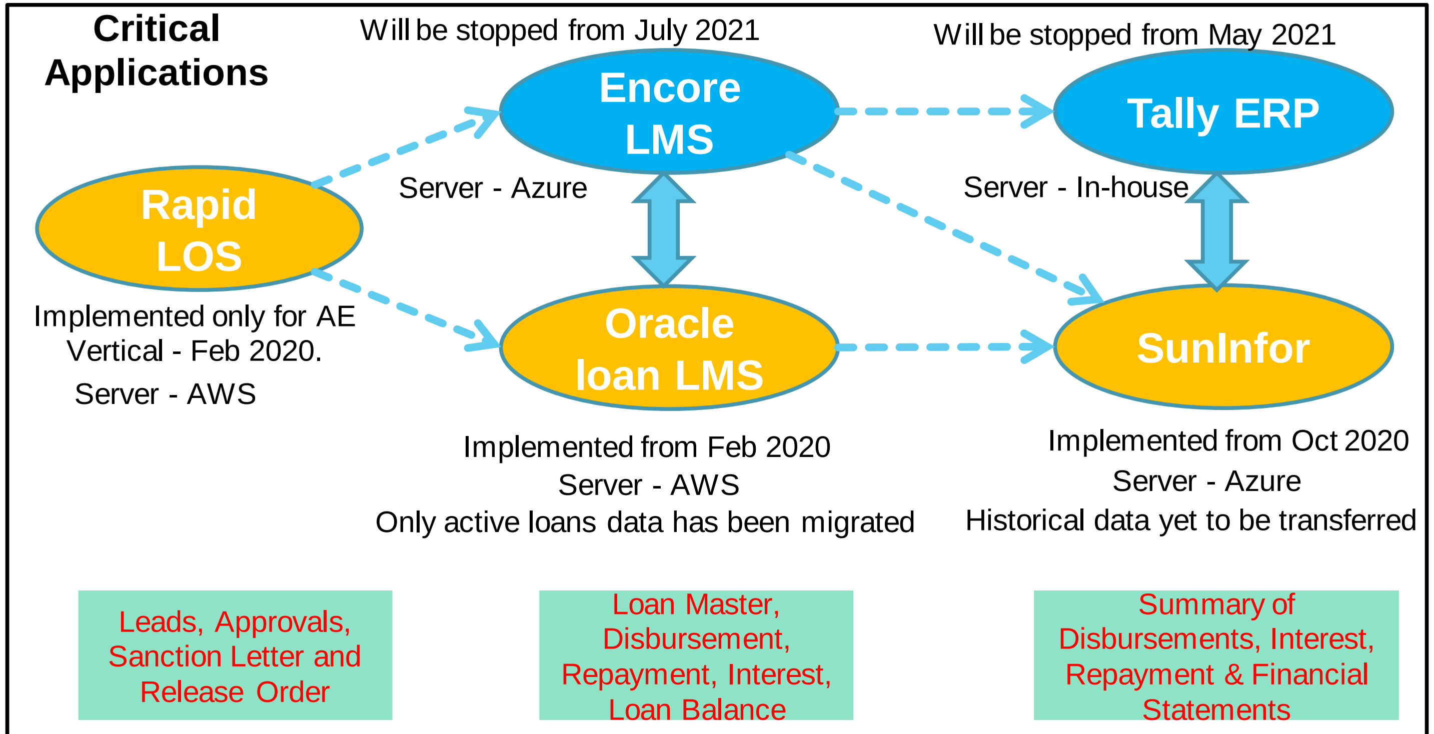
Manual Data Transfer	⇢
Automated Data Transfer	→

Business Process	MRP	Vendor Master	Purchase Order	Goods Inward	Accounts Payable & Accounting
Procurement of Direct Material	App 1	App 1	App 1	App 1	App 1

Business Process	Vendor Master	Budget	Purchase Order	Goods Inward	Data Transfer	Accounts Payable & Accounting
Procurement of Indirect Material	App 1	App 2	App 2	App 2		App 1 (Manual updation/Keying in of transactions)

Business Process	Goods Inward	Quality Acceptance	Issue to Production	Inventory Valuation	Production Recording and Consumption
Inventory of Direct Materials	App 1 (Direct Materials)	App 1 (Direct Materials)	App 1	App 1	App 1 (Manual updation/Keying in of transactions)

2c. Illustrative IT Application Landscape – NBFC


Critical Applications
Will be stopped from July 2021
Will be stopped from May 2021
Encore LMS
Tally ERP
Rapid LOS
Server - Azure
Server - In-house
Implemented only for AE Vertical - Feb 2020.
Server - AWS
Oracle loan LMS
SunInfor
Implemented from Feb 2020
Server - AWS
Only active loans data has been migrated
Implemented from Oct 2020
Server - Azure
Historical data yet to be transferred
Leads, Approvals, Sanction Letter and Release Order
Loan Master, Disbursement, Repayment, Interest, Loan Balance
Summary of Disbursements, Interest, Repayment & Financial Statements

Note:

- Single Sign on yet to be implemented for Key Applications
- Integrated of LOS, LMS and Accounting system (and banking channel) is yet to be done

Support Apps - Business

Document Management System	MS Office 365
Deferral Tracking System (*)	Power BI - MIS
Integrated Document Admin. Sys. (IDAS) (*)	Operations Service Desk (*)
Legal Management System (*)	Risk Management System (*)
Iassign (*)	Tracker PAL

Support Apps - IT

Change Management System (*)	Task Management System (*)
Incident Management System (*)	Asset Management System (*)

Support Apps – HR & Payroll

Hi Note (Employee self service portal)	Metrics (Biometric), Dockabl (Metrics)
LinkedIn Learning (Employee Training)	Zing HR (*)

Legend : New Application | Old Application

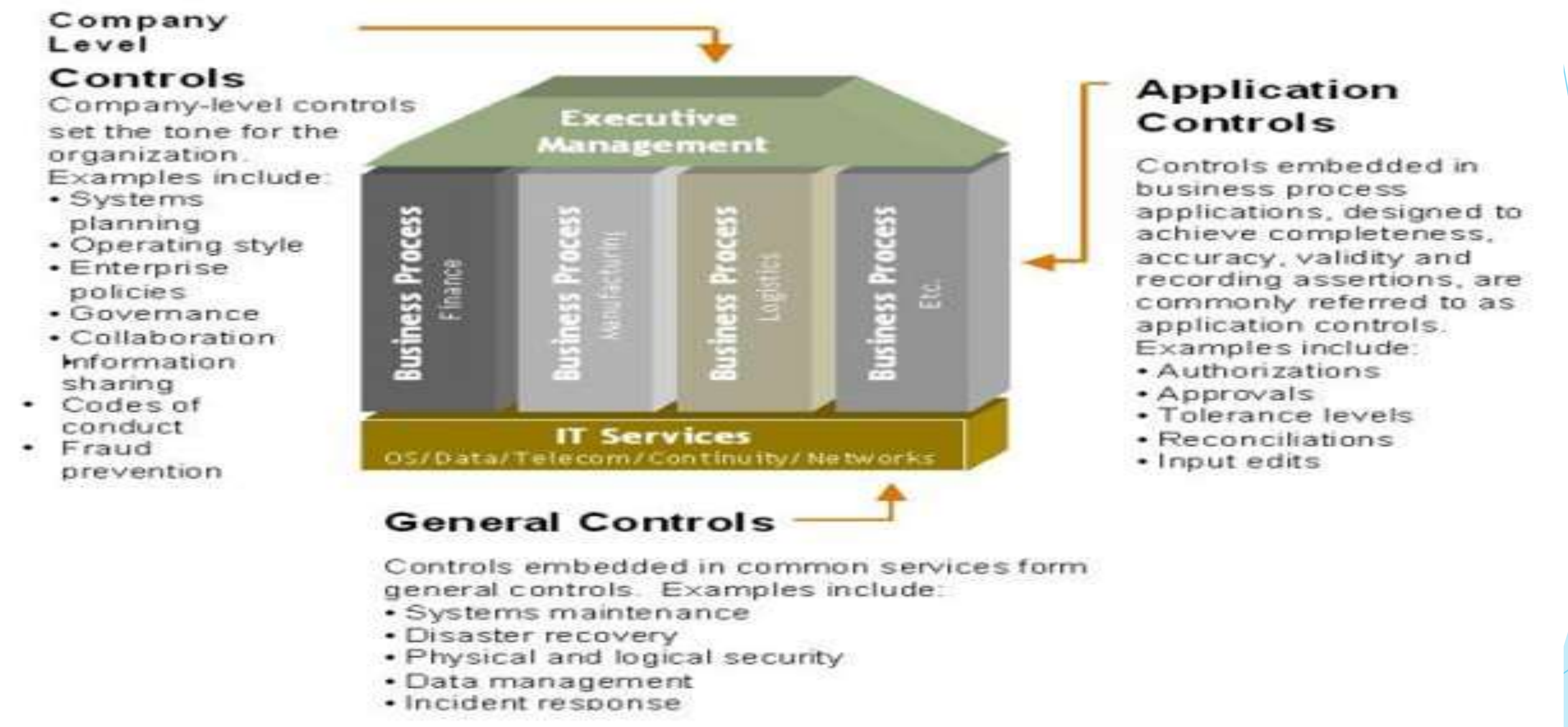
🟩 Data

- - ➤ Not integrated

⇔ Parallel Implementation

(*) – Applications accessible through Single Sign-on

2d. Common elements of IT Control



Company Level Controls

Company-level controls set the tone for the organization. Examples include:

- Systems planning
- Operating style
- Enterprise policies
- Governance
- Collaboration
- information sharing
- Codes of conduct
- Fraud prevention

Application Controls

Controls embedded in business process applications, designed to achieve completeness, accuracy, validity and recording assertions, are commonly referred to as application controls. Examples include:

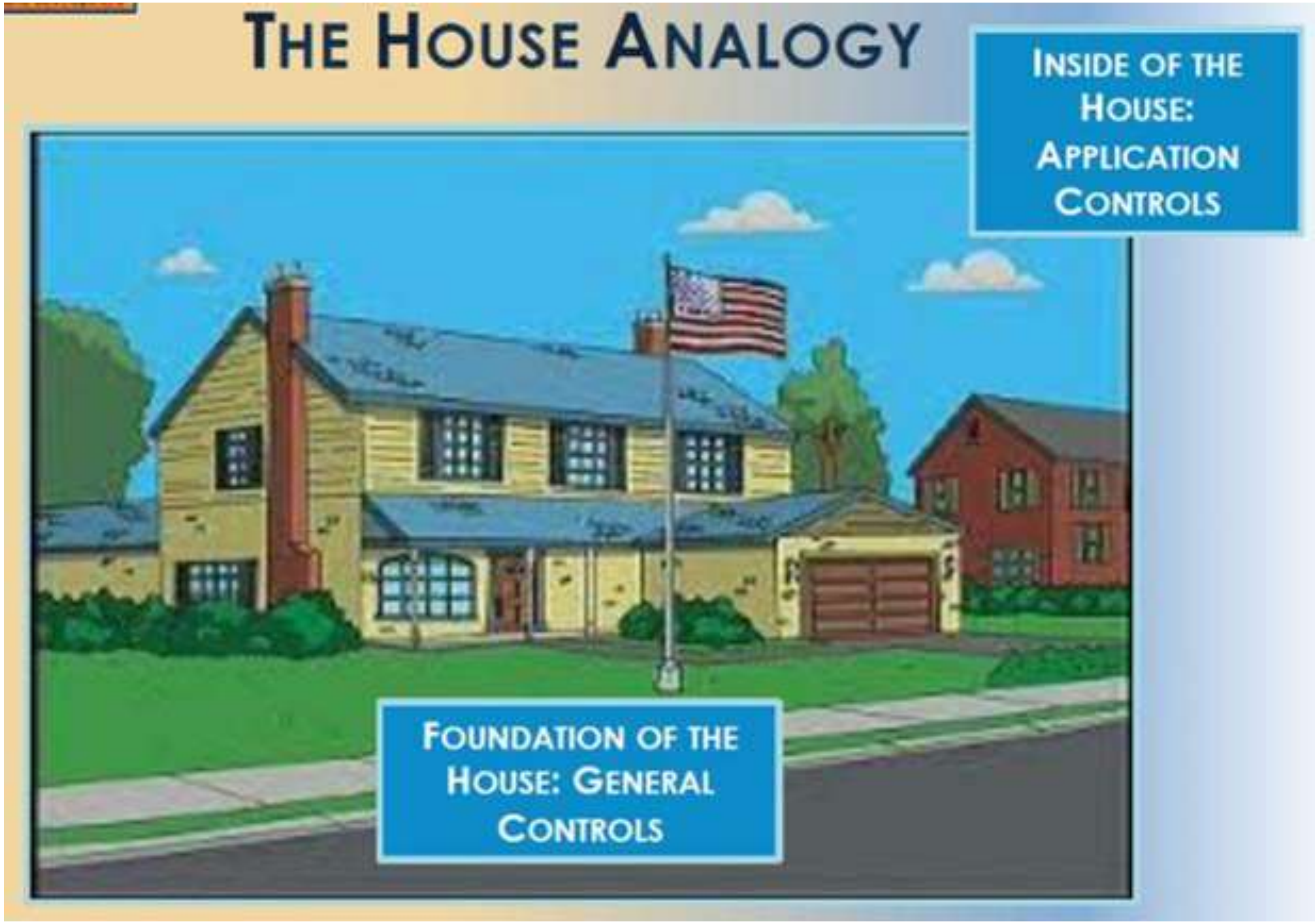
- Authorizations
- Approvals
- Tolerance levels
- Reconciliations
- Input edits

General Controls

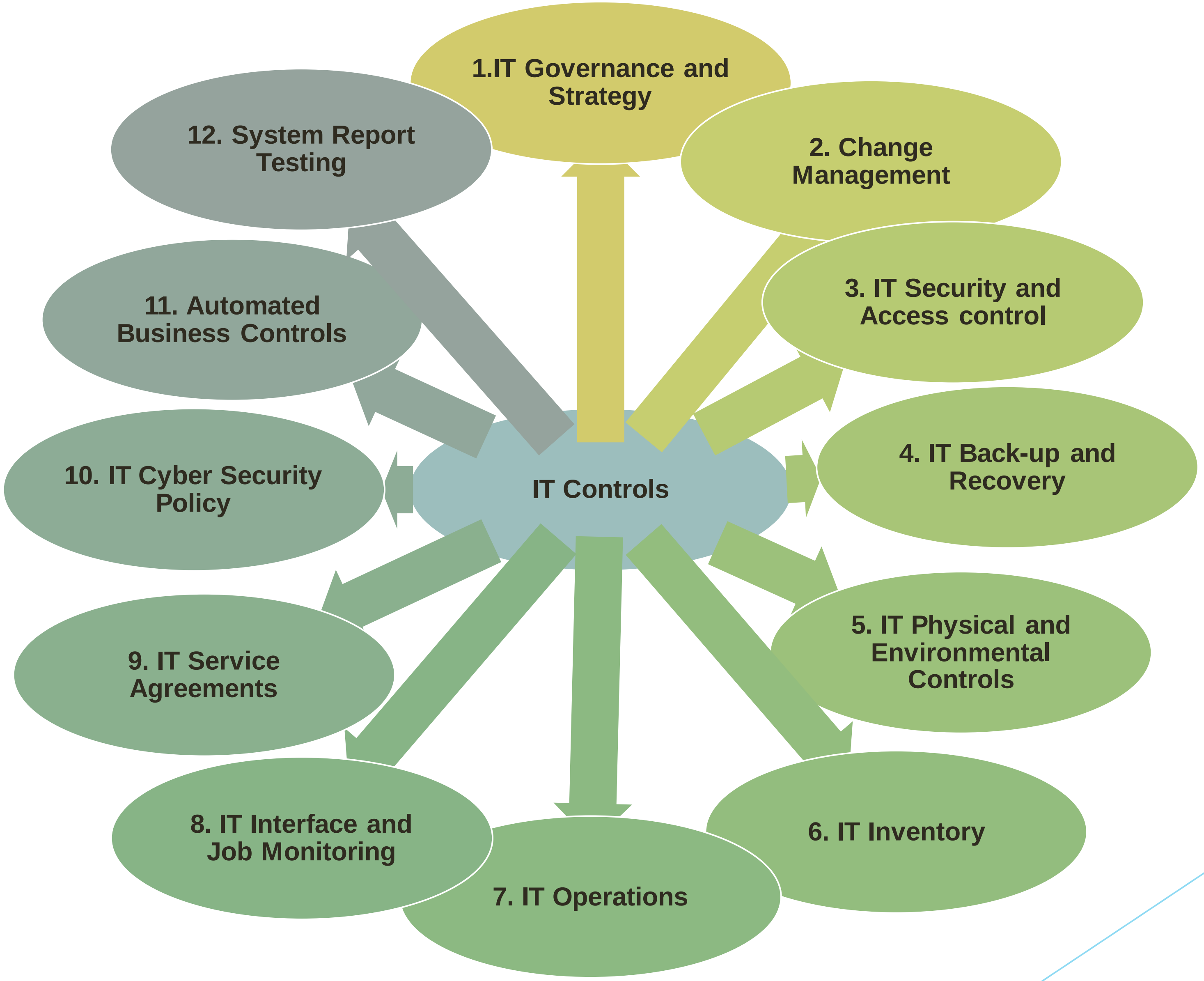
Controls embedded in common services form general controls. Examples include:

- Systems maintenance
- Disaster recovery
- Physical and logical security
- Data management
- Incident response

2d. IT General Controls vs IT Application Controls


THE HOUSE ANALOGY
INSIDE OF THE HOUSE: APPLICATION CONTROLS
FOUNDATION OF THE HOUSE: GENERAL CONTROLS

2e. IT Controls – Key Domains


IT Controls
1.IT Governance and Strategy
2. Change Management
3. IT Security and Access control
4. IT Back-up and Recovery
5. IT Physical and Environmental Controls
6. IT Inventory
7. IT Operations
8. IT Interface and Job Monitoring
9. IT Service Agreements
10. IT Cyber Security Policy
11. Automated Business Controls
12. System Report Testing

2e. IT Controls – Key Domains

IT Governance and Strategy

IT Strategy, alignment with business objectives, IT Organization Structure, IT Budgeting, review of system implementation, approved policies and procedures, measurement through KPIs

Change Management

a) Changes are approved and tested before being moved to Production environment

b) Access to make change-restricted and Segregated

c) Post Implementation Review by management

Refer Annexures for further details

IT Security and Access control

a) Existence of IT Security Policy (including awareness session)

b) Access (including Privileged Access) is approved

c) Unique User IDs are assigned (and if generic IDs are used, compensating controls should be in place)

d) Access to terminated users removed in timely manner

e) Password Controls put in place

f) System Activity is logged

Refer Annexures for further details

IT Backup and Recovery

Documented Procedures, Monitoring of data back up, Periodic testing of back up (assessment of critical and non critical data to be done for the purpose of Disaster Recovery)

Refer Annexures for further details

2e. IT Controls – Key Domains

IT Physical and Environmental Controls

Only authorized users have access to data center, access to data center is monitored, environment control like, raised ceiling, humidity controls, smoke detection and automatic fire-extinguishing equipment is installed for protection against fire hazards.

IT Inventory

a) Inventory of Hardware and Software to be maintained

b) Control on unused equipment, AMC for existing assets, disposal as per e-waste regulations, data security

Refer Annexures for further details

IT Operations

Issues are handled effectively (as per SLAs), Roles and Responsibilities are clearly defined, real time monitoring of network and server utilization

IT Interface and Job Monitoring

Access to update batch Jobs Restricted, system interfaces are periodically monitored

2e. IT Controls – Key Domains

IT Service Agreements

SLAs should be formally documented and measured, Contracts to include key terms like confidentiality, right to audit etc,

IT Cyber Security Policy

a) Cyber Security Risk Assessment to be done by IT Administration

b) Antivirus, DLP (Data Loss/ Leakage Prevention), and other Applications is updated on a monthly basis.

c) Control on remote access

Automated Business Controls

Comprises of business cycle controls that are configured in the application. Some examples include Data entry and validation controls, Reasonable checks and logics, Completeness checks, Logical security/ access controls, Segregation of duties, Pre-and-post implementation audits, including audit of new system and controls (e.g. GST implementation, CRM, CBS, SRM, RPA, Blockchain, etc.)

System Report Testing

Covers test logic, completeness and accuracy of reports is covered

Questions

- An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to:

  A. Meet business objectives

  B. Enforce data security

  C. Be culturally feasible

  D. Be financially feasible

- From a control perspective, the PRIMARY objective of classifying information assets is to:

  A. establish guidelines for the level of access controls that should be assigned.

  B. ensure access controls are assigned to all information assets.

  C. assist management and auditors in risk assessment.

  D. identify which assets need to be insured against losses.

Questions

- 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.

- The communication lines are strictly drawn between the Chief Information Officer and Chief Financial Officer so as to maintain the _________ of the data within the application

  A. Confidentiality

  B. Integrity

  C. Availability

  D. All the above

Questions

- 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

- General IT controls are known as ______controls

  A. Pervasive

  B. Indirect

  C. Both A & B

  D. None of the above

SIA - 530

3a. Introduction to SIA 530

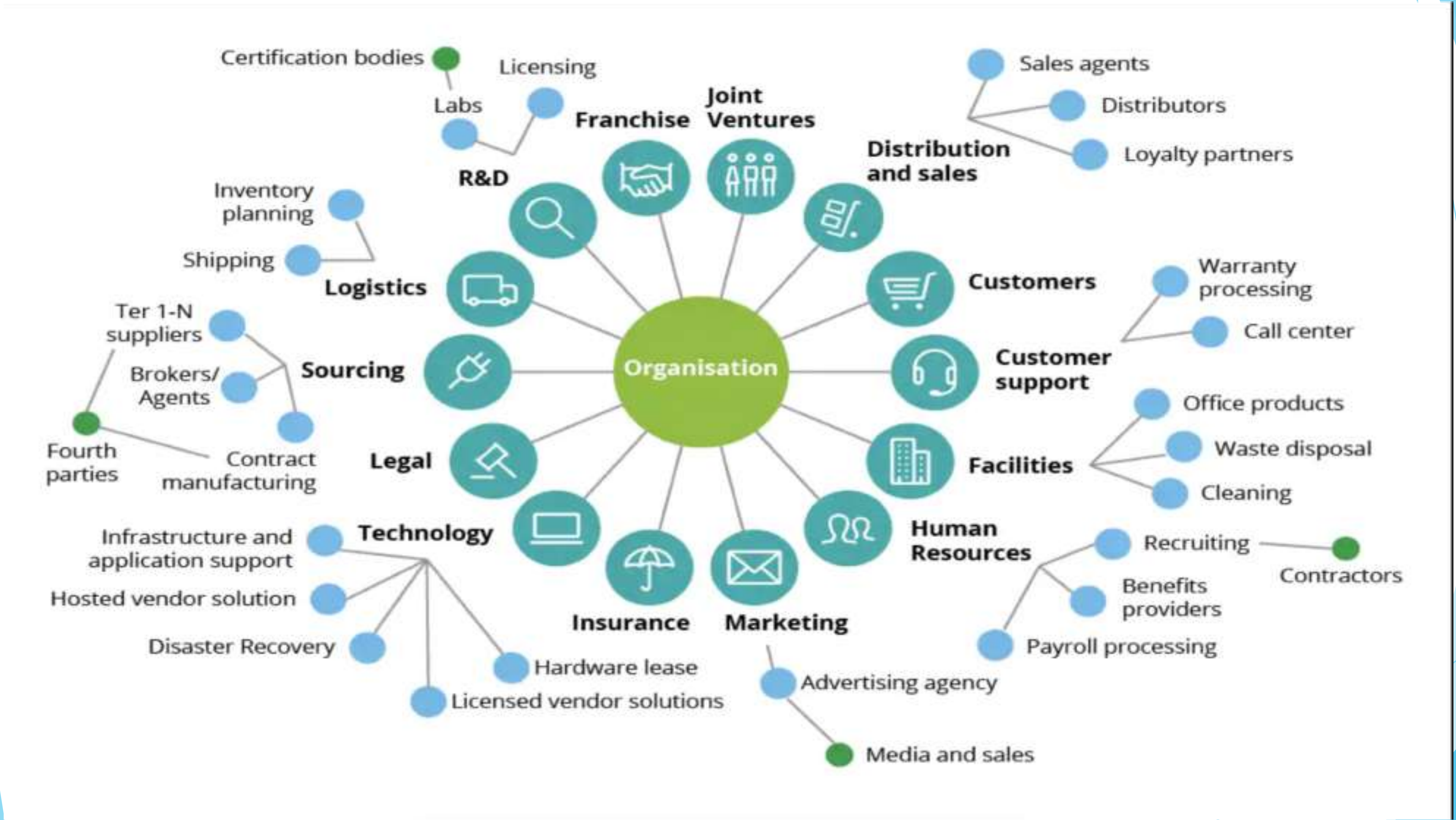
- This Standard deals with the **responsibility of the Internal Auditor** and management with regard to risks arising from situations where some parts of the entity's business operations, processes and information **reside with Third-Party Service Providers (TPSPs)**

- **Meaning of TPSPs** - They are External outsourced service provider to whom either full or some aspect of business function, operation or processing or activity is outsourced.

- The **Landscape of Third Party Services** is provided in the subsequent slide.

- **Risks relating to Outsourcing** - Business processing, Financial and operational management,, Information security, Legal compliance and Business continuity

3b. Third Party Services Landscape



3c. Objectives of the Standard

- The primary objective of this Standard is to prescribe the key requirements for providing an independent assurance over business Standard On Internal Audit (SIA) 530 2 operations at third party service providers.
- These requirements are in the nature of
  - ❑ Assessment of risks associated with outsourcing, Evaluation of adequacy of controls to address risks of errors and irregularities, Cost and operational efficiencies and ensuring compliance with IT policies and standards, as well as contractual, statutory and regulatory requirements.
  - ❑ To ensure quality independent audit reports on TPSP’s Controls.
  - ❑ To prescribe requirements for the Internal Auditor in evaluating the TPAA report provided by an Independent Auditor covering effectiveness of outsourced processes

3d. Requirements/Audit Procedure

Internal Auditor shall:

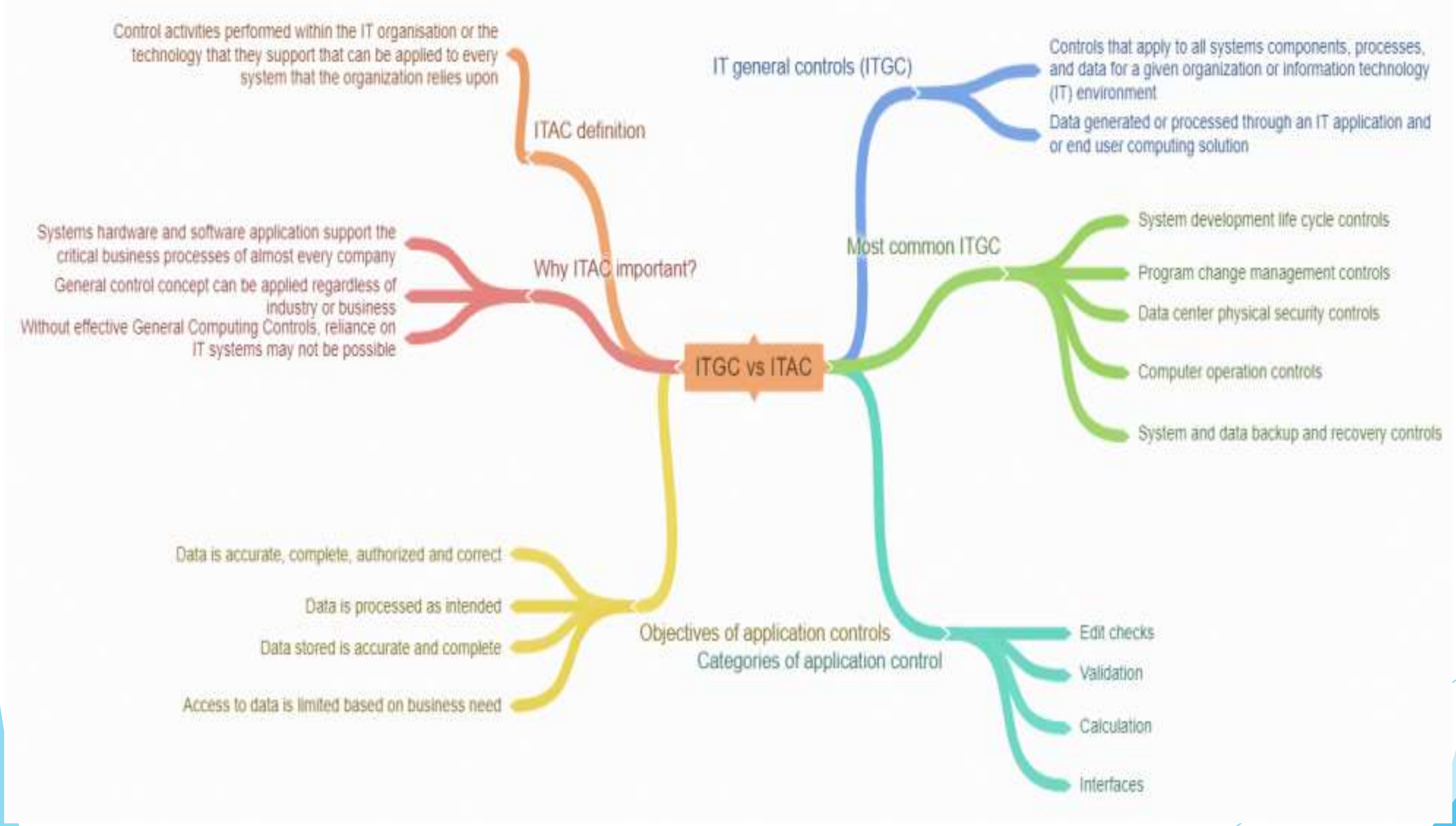
1. Study and **evaluate the scope of TPSP's services**, governance and oversight process (Database of Outsourced Services, SLAs (vetted by legal), roles and responsibilities of user entities officials.
2. Review both, the **Pre-engagement and Post engagement** due diligence undertaken by the User Entity, including an assessment of the control environment at the TPSP
3. Review the **periodic independent risk assessment** of each third-party arrangement conducted by the management
4. The Internal Auditor shall conduct an independent audit of the TPSP (where permissible), which shall include TPSPs' entity's level controls, IT controls and process controls
5. In case, the Internal Auditor is not performing an independent audit but obtains TPAA reports, the review of the TPAA reports shall be undertaken in compliance with Standard on Internal Audit (SIA) 240

Thank you

CA Rekha Surana
rekhasurana@gmail.com

Annexures

Common elements of IT Control



ITGC vs ITAC

ITAC definition

Control activities performed within the IT organisation or the technology that they support that can be applied to every system that the organization relies upon

Why ITAC important?

Systems hardware and software application support the critical business processes of almost every company

General control concept can be applied regardless of industry or business

Without effective General Computing Controls, reliance on IT systems may not be possible

Objectives of application controls

Data is accurate, complete, authorized and correct

Data is processed as intended

Data stored is accurate and complete

Access to data is limited based on business need

IT general controls (ITGC)

Controls that apply to all systems components, processes, and data for a given organization or information technology (IT) environment

Data generated or processed through an IT application and or end user computing solution

Most common ITGC

System development life cycle controls

Program change management controls

Data center physical security controls

Computer operation controls

System and data backup and recovery controls

Categories of application control

Edit checks

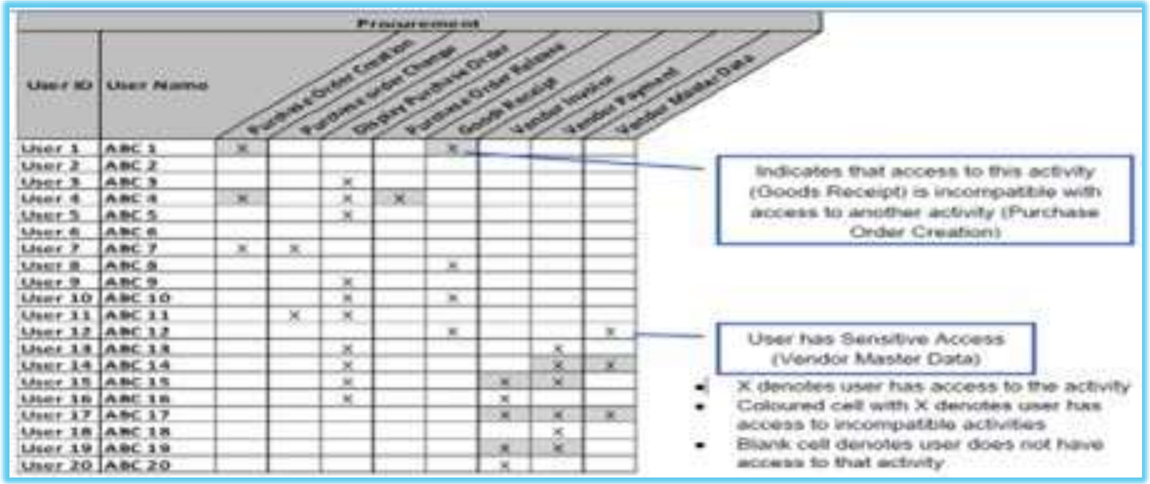
Validation

Calculation

Interfaces

Logical Access Control

Privileged user access management



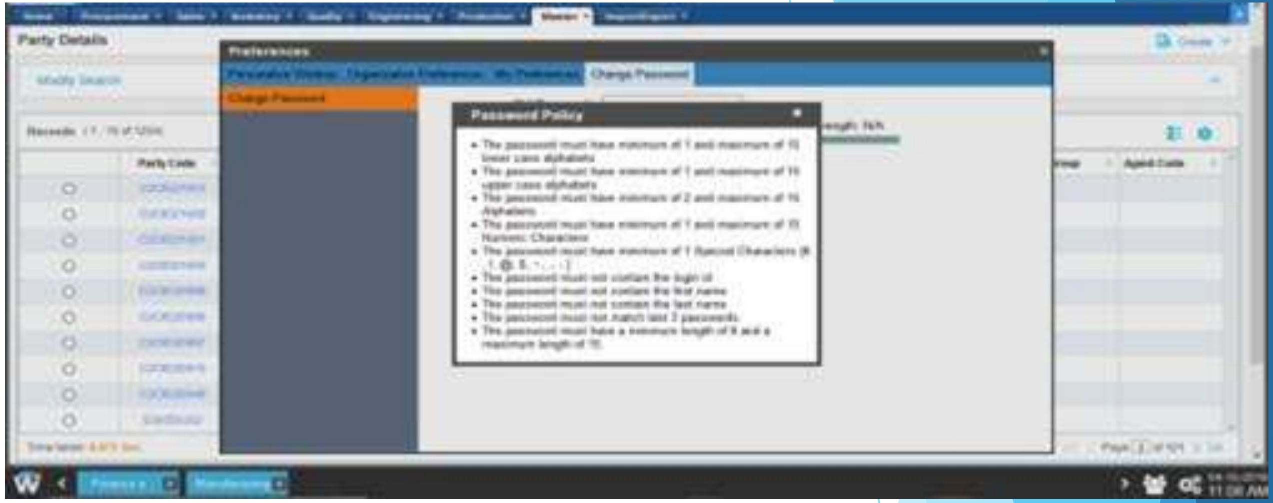
		Procurement							
User ID	User Name	Purchase Order Creation	Purchase order Change	Display Purchase Order	Purchase Order Release	Goods Receipt	Vendor Invoice	Vendor Payment	Vendor Master Data
User 1	ABC 1	X				X			
User 2	ABC 2								
User 3	ABC 3			X					
User 4	ABC 4	X		X	X				
User 5	ABC 5			X					
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)

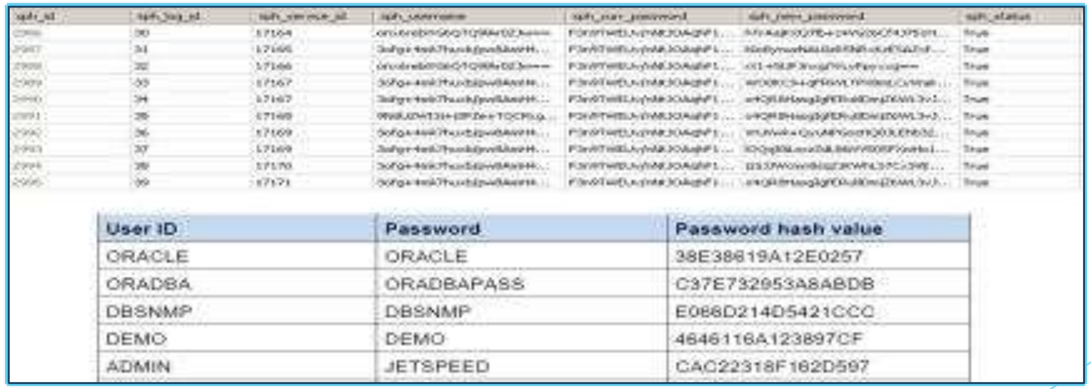
- X denotes user has access to the activity
- Coloured cell with X denotes user has access to incompatible activities
- Blank cell denotes user does not have access to that activity

Password Configuration



- 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 (# ! @ $ [illegible])
- 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.

Encryption

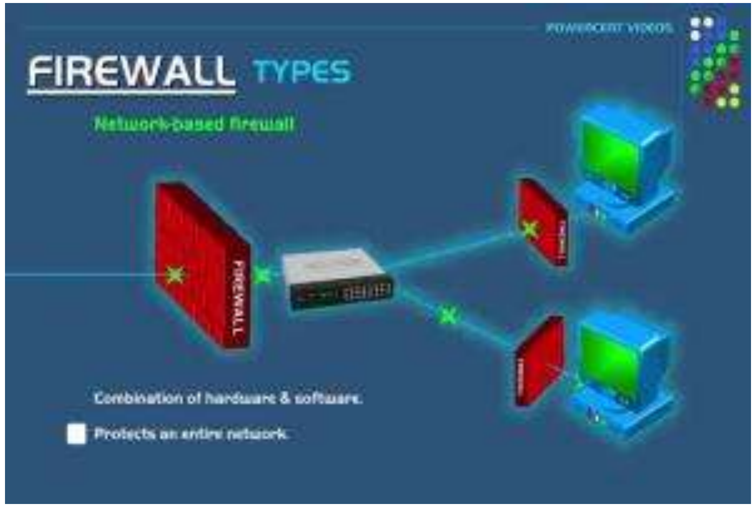


sph_id	sph_log_id	sph_service_id	sph_username	sph_curr_password	sph_new_password	sph_status
2986	30	17164	[illegible]	[illegible]	[illegible]	True
2987	31	17165	[illegible]	[illegible]	[illegible]	True
2988	32	17166	[illegible]	[illegible]	[illegible]	True
2989	33	17167	[illegible]	[illegible]	[illegible]	True
2990	34	17167	[illegible]	[illegible]	[illegible]	True
2991	35	17168	[illegible]	[illegible]	[illegible]	True
2992	36	17169	[illegible]	[illegible]	[illegible]	True
2993	37	17169	[illegible]	[illegible]	[illegible]	True
2994	38	17170	[illegible]	[illegible]	[illegible]	True
2995	39	17171	[illegible]	[illegible]	[illegible]	True

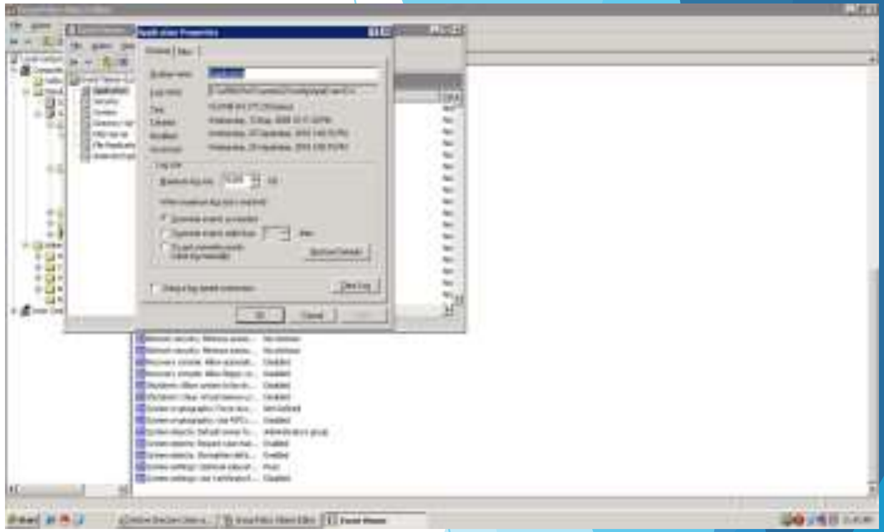
User ID	Password	Password hash value
ORACLE	ORACLE	38E38619A12E0257
ORADBA	ORADBAPASS	C37E732953A8ABDB
DBSNMP	DBSNMP	E066D214D5421CCC
DEMO	DEMO	4646116A123897CF
ADMIN	JETSPEED	CAC22318F162D597

Information Security

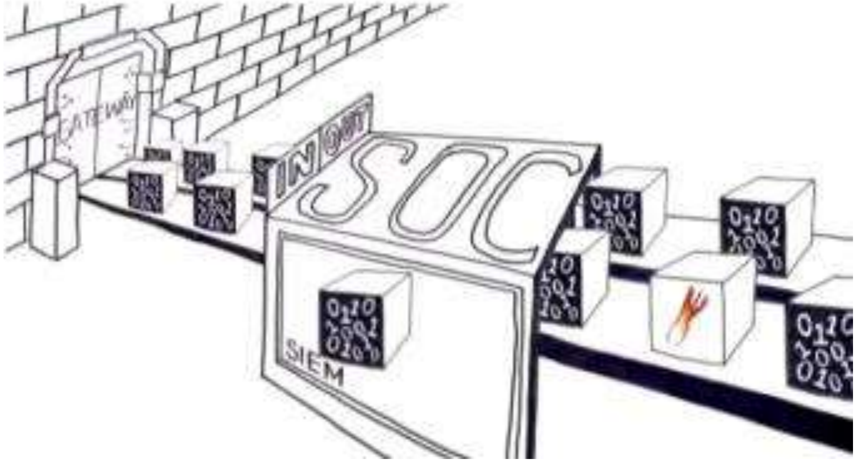
Firewall


POWERCERT VIDEOS
FIREWALL TYPES
Network-based firewall
FIREWALL
Combination of hardware & software.
Protects an entire network.

Server Performance

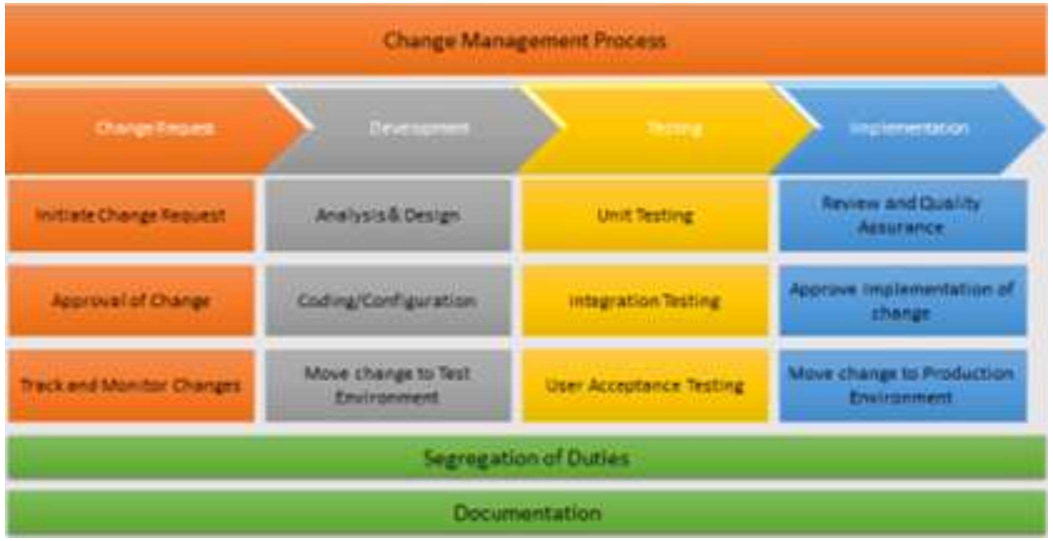


SOC



Change Management

Change Management Process



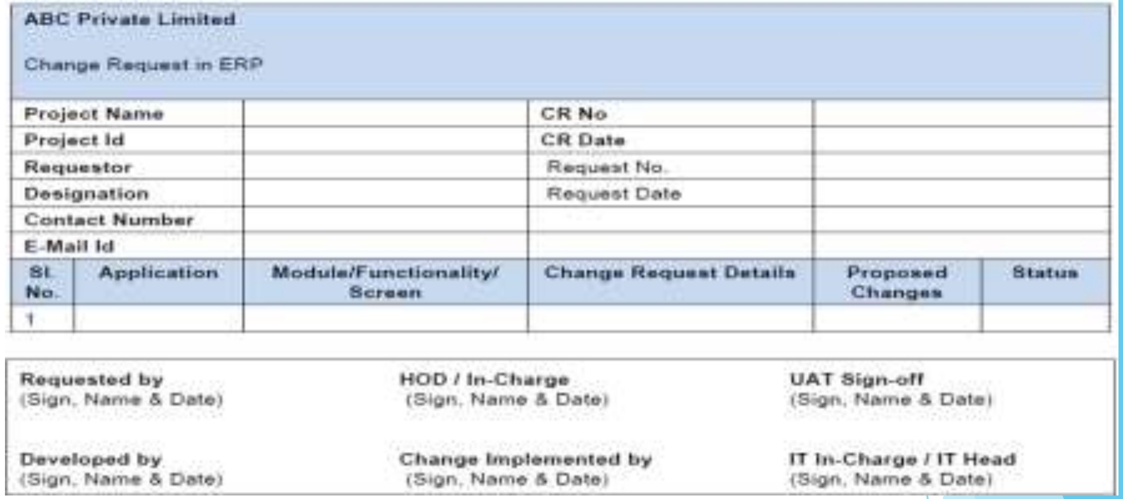
Change Management Process

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

Change Request



ABC Private Limited

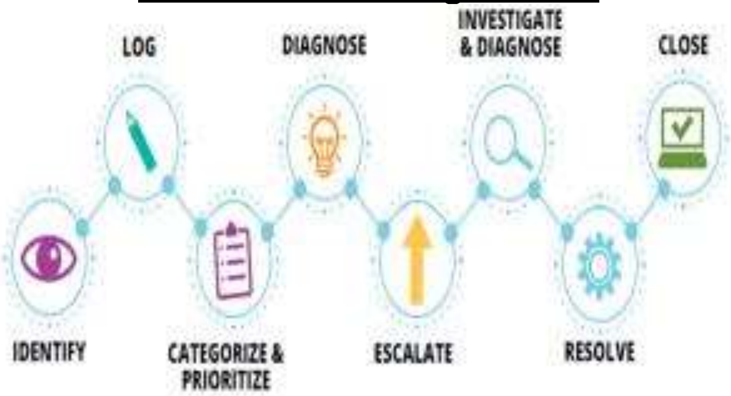
Change Request in ERP

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					

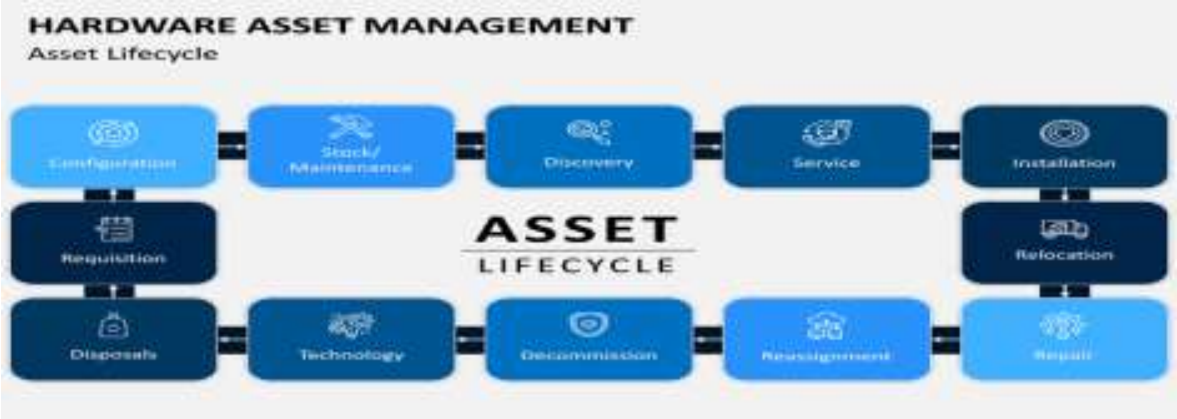
Requested by (Sign, Name & Date)	**HOD / In-Charge** (Sign, Name & Date)	**UAT Sign-off** (Sign, Name & Date)
Developed by (Sign, Name & Date)	**Change Implemented by** (Sign, Name & Date)	**IT In-Charge / IT Head** (Sign, Name & Date)

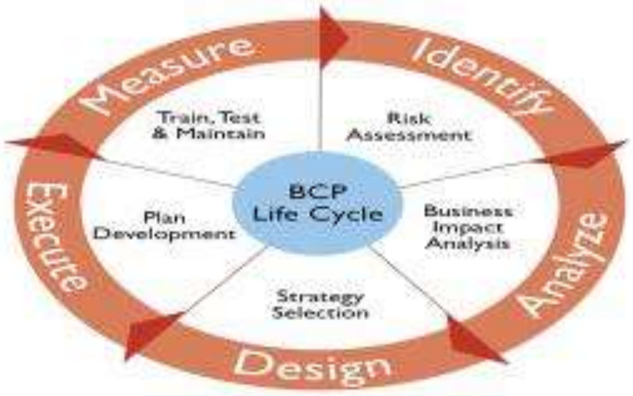
Incident Management



Asset Management and Backup

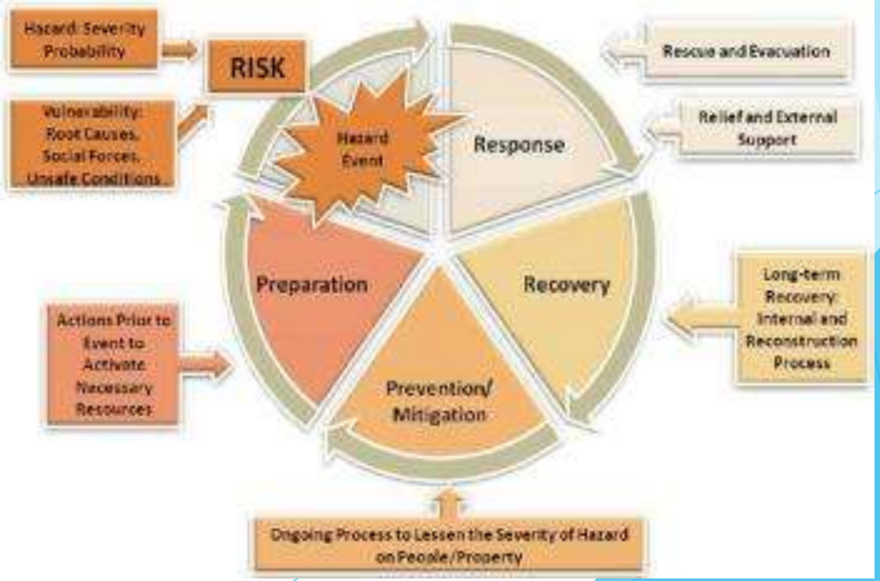
5. Asset Management – Hardware and Software





6. Backup

- Content
- Frequency
- Storage
- Restore
- Restricted access


Hazard: Severity Probability
RISK
Vulnerability: Root Causes, Social Forces, Unsafe Conditions
Hazard Event
Response
Rescue and Evacuation
Relief and External Support
Preparation
Recovery
Long-term Recovery: Internal and Reconstruction Process
Actions Prior to Event to Activate Necessary Resources
Prevention/ Mitigation
Ongoing Process to Lessen the Severity of Hazard on People/Property