

Types of Systems Audit & Relevance

Presented By:
Prasad Pendse, CISA



Agenda

- ✓ Systems Audit
- ✓ Categories & Types of Systems Audit, Relevance
 - ❑ IT & Application Audits
 - ❑ Security Audits
 - ❑ Process Audits
 - ❑ Compliance Audits
- ✓ Advantages of Systems Audit
- ✓ Professional Qualifications for Systems Audit

Systems Audit

Introduction:

- An audit of the controls designed and implemented into the system to ensure the integrity of the data processed by the system and maintain the proper functionality of system processes.

System Audit Categories:



Relevance:

- Provide assurance that IT Systems are adequately protected
- Reduce risk of data tampering, data loss or leakage, service disruption and poor management of IT systems

Types of Systems Audit

ITGC Controls
Review

Application Audit

System Interface
Audit

Pre-Implementation
Review

Post-
Implementation
Review

Security Audit

Data Centre Audit

Third party
Information Risk
Assessment

Process Audit

Data Migration
Audit

Performance Audit

Statutory Audit

Internal Controls
Review / SOX
Controls Review

SAS70/SSAE16/ISAE
3402 audit of IT
Processes

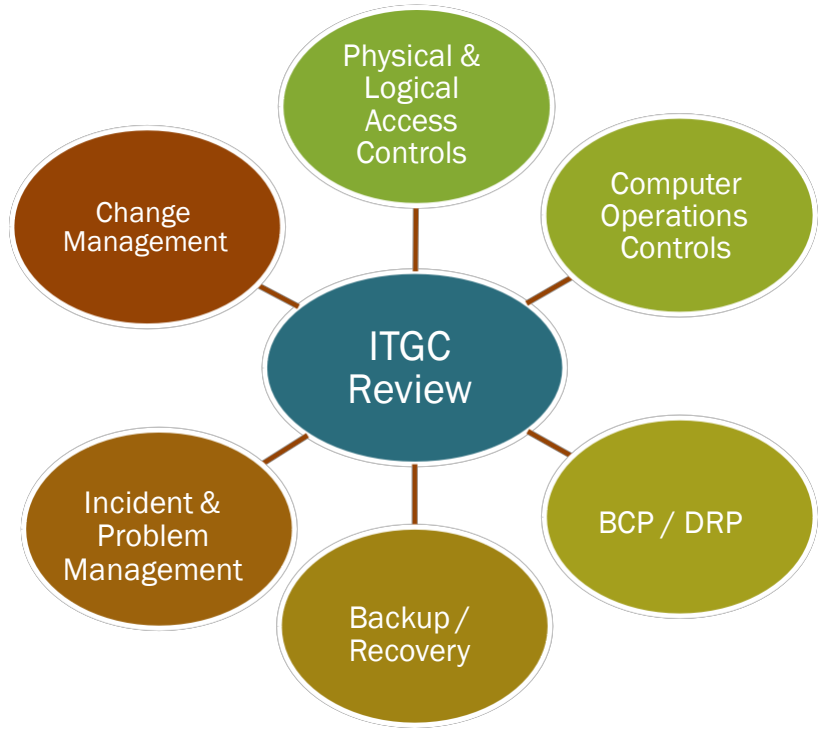
Software Asset
Management (SAM)
Audit / Licensing
Audit

IT General Controls (ITGC) Review

Introduction:

- An audit of the controls in place for technology that affects the management of fundamental organizational processes.

ITGC Areas:



Relevance:

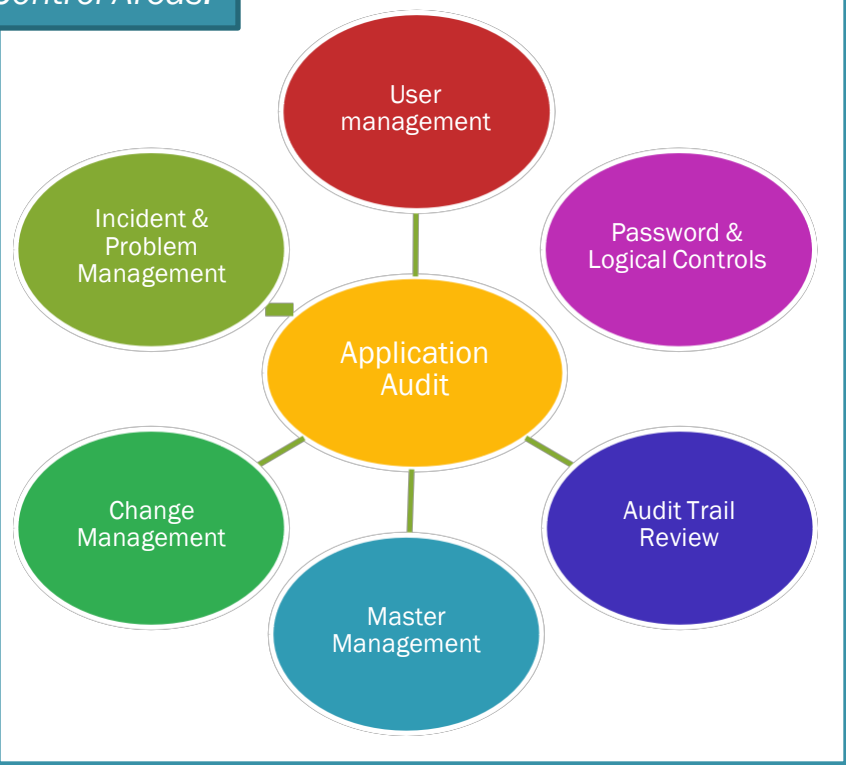
- Ensure the proper development and implementation of applications
- Integrity of programs, data files, and computer operations.

Application Audit

Introduction:

- According to ISACA, “The policies, procedures and activities designed to provide reasonable assurance that objectives relevant to a given automated solution (application) are achieved.”

Control Areas:



Relevance:

- Changing nature of Business
- Data accuracy
- Completeness
- Validity, verifiability and consistency
- Achieve data integrity and data reliability

System Interface Audit

Introduction

- Exchange of information between two or more applications.
- Requires data validation for input as well as output controls

Relevance:

- Complexity of IT Infrastructure and system interfaces for information flow
- Risks associated with Data Integrity
- Eavesdropping

Pre-Implementation Review

Introduction:

- Audit review of a system currently being developed.
- To evaluate and test proposed control environment in the new system

Relevance:

- The IT solution meets the business requirements.
- BU and IT are aware of controls needed within the system.
- Managed effectively and efficiently during design, development and implementation.
- Implemented in accordance with established policies and best practices.

Post-Implementation Review

Introduction:

- Evaluates whether the project has achieved its intended objectives,
- Reviews the performance of project management activities and captures learning points for future improvements

Relevance:

- Ensure that the original requirements have been successfully implemented into production.
- Review is not limited for completion of project but to ensure that the organization benefits from the project outcome.

Security Audit

Introduction:

- Systematic evaluation of the security of a company's information system by measuring how well it conforms to a set of established standards / criteria.
- Classified as Internal & External Security Audit

Audit Areas:



Relevance:

- Security systems and processes are working as intended
- Comply with the legislations and acts
- Identify the gaps in the existing defenses
- Complex nature of systems
- Hacking incidents / breach

Data Centre Audit

Introduction:

- Comparing existing infrastructure against best industry practices and it mainly includes review of Physical and environmental security.

Relevance:

- Large investments in Data & Hardware
- Complex IT Architectures
- Data Center Tier Levels based on criticality

Third Party Information Risk Assessment

Introduction:

- Review of business functions and operations to determine whether the activities, resources and behaviors are being managed efficiently and effectively.
- Results of business operations and measures them against the predetermined goals of the company.

Relevance:

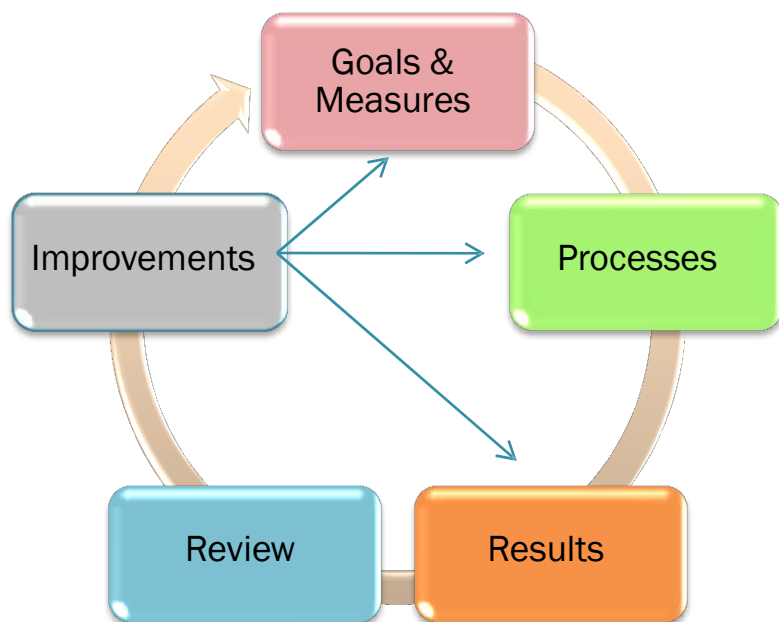
- Compliance risk for third party business relationships
- Reduced data loss
- Applicable Standards: ISO 27001, SSAE 16, etc.

Process Audit

Introduction:

- Review of business functions and operations to determine whether the activities, resources and behaviors are being managed efficiently and effectively.
- Results of business operations and measures them against the predetermined goals of the company.

Effective Management of Process:



Relevance:

- Standardization of processes
- Quality Standards such as ISO 9000
- Non core activities outsourced to third party

Data Migration Audit

Introduction:

- Data Migration audit verifies the completeness & accuracy of data transferred from legacy system to new system.

- Focus on:
 - Completeness
 - Accuracy
 - Consistency

Relevance:

- Technological advancement, legacy systems, efficient newer systems

- Consistency of data migrated to new system

Performance Audit

Introduction:

- Refers to an examination of a program, function, operation or the management systems and procedures.
- Review of systems (hardware, software, network) performance over period.

Relevance:

- Helps in detecting frauds, performance deviations.
- Future requirement to support future growth

Compliance / Statutory Audit

Introduction:

- Compliance audits provide management with tool for the internal review of compliance in their operating units.
- Is governed by respective statutes, laws& rules.

Relevance:

- Changing nature of business resulting In statutory changes across the World
- Standardization of business processes for the critical, financially relevant systems.

Compliance / Statutory Audit (cont...)

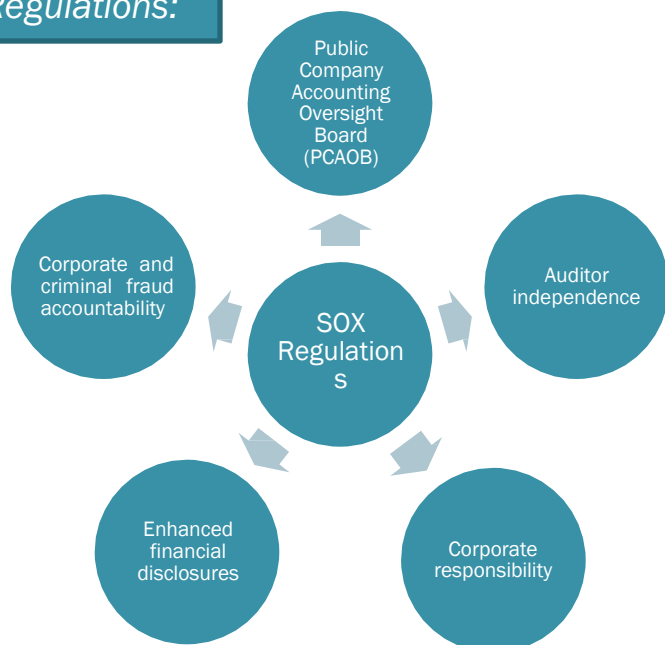
#	Audit Name	Regulator/ Authority	Entity	Circular No.	Frequency	Professional Qualification
1	System Audit	RBI	RBI, Banks, NBFC's	RBI/2010-11/494 DBS.CO.ITC.BC.No.6/31.0 2.008/2010-11	NBFC: Yearly RBI, Banks	CISA/CISSP/CIS M/DISA
2	System Audit	SEBI	Stock Exchange, MF's, Stock brokers	CMTR23912, MCX- SX/CTCL/1101/2013, CMTR23125	Annually	CISA/CISM/DISA
3	Code of Practice for Metering & Billing (CPMBA)	TRAI	Telecom Companies	F.No.302-1/2010-QoS	Yearly	CA's
4	Investment Risk Management system & Process Audit	IRDA	Insurance Companies	IRDA-INV/CIR/023/2009- 10	3 years	CA's
5	System Audit	IT Act 2000		IT Act 2000		
6	SSAE16	AICPA	Service Organizations	Auditing std. board(ASB) of AICPA	Yearly	CPA's
7	Internal controls & Financial Reporting	SOX Act, USA	Listed companies in USA & their subsidiaries.	SOX Act	Periodically	CPA's
8	System Audit	PCI-DSS	Payment Card industry	Contractual Requirement for Payment card service provider	As per requirement	PCI-QA

Internal Control Review / SOX Control Review / Clause 49

Introduction:

- The Sarbanes-Oxley Act (SOX) defines the requirements for the integrity of source data related to financial transactions and disclosures.
- SOX Section 404 – implementation of technical controls and continuous access auditing to assure the reliability of data related to financial transactions.
- Clause 49 (Indian equivalent of SOX) which states top management becomes directly accountable for all financial statements and internal controls of the organization

SOX Regulations:



Relevance:

- Corporate scandals and lack of investor confidence
- Significance to Corporate Governance
- High penalties for management of Companies & imprisonment



SAS70 / SSAE16 / ISAE 3402 Audit of IT Processes

Introduction:

- Statement on Standards for Attestation Engagements (SSAE) No. 16 - The standard for service organizations to demonstrate controls in operations and its design to achieve objectives set forth.
- Attested by an Independent Auditor. The standard provides for two types of reporting Type I and Type II.

Relevance:

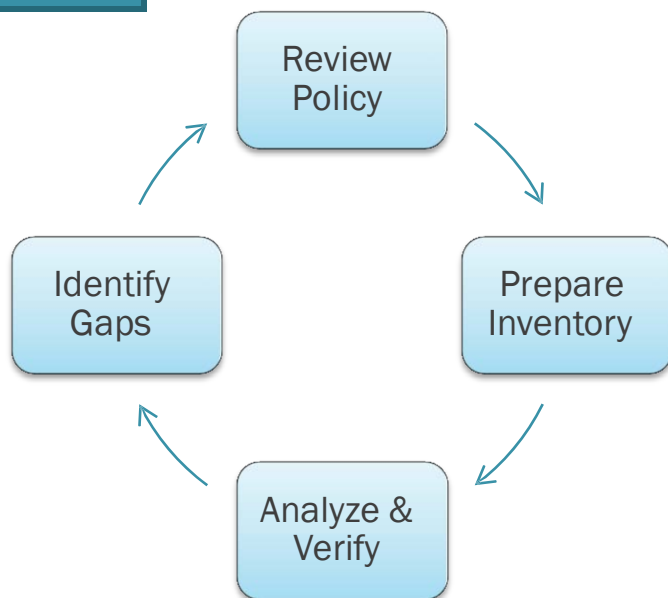
- Need for written assertion from management of service organization regarding effectiveness of controls
- Outsourcing of non-core activities affecting financials of parent company
- “Attest” function than SAS70’s “Audit” function

Software Asset Management (SAM) Audit / Licensing Audit

Introduction:

- SAM audit involves review of following business practices for software application within organization

Activities:



Relevance:

- Complex licensing requirements
- High cost of Licensing
- Unrestricted use of internet by employees

Advantages of System Audit

Advantages:

- Detection of non compliant procedure
- Continual Improvement
- Increase in productivity
- Increased Confidentiality, Integrity & Availability
- Increased data accuracy, completeness, validity, verifiability and consistency
- Build a confidence among stakeholders through increase in safe & secure system
- Compliance to Statutory / Compliance / Legal Requirements

Qualifications for System Audit

Qualification	Certification Body*
Certified Information Systems Auditor (CISA)	
Certified Information Security Manager (CISM)	
Diploma in Information System Audit (DISA)	
Global Information Assurance Certification (GIAC)	
Certified Information Systems Security Professionals (CISSP)	
Systems Security Certified Professionals (SSCP)	
Certified in Risk & Information Systems Control (CRISC)	
ISO 27001:05 Lead Auditors (LA)	

* Logo's have been taken from websites of the respective Organizations.

Agility | Precision | Quality

talk to us!

Prasad Pendse