Overview of Information System Security & Audit

(Chapter -1 : DISSA Course) **- session 2 & 3**

Arijit Chakraborty

15th & 16th May 2021

TOP 5 FRAUD SCHEMES
CURRENTLY OBSERVED DUE TO THE CORONAVIRUS

CYBERFRAUD

83% OVERALL INCREASE | **47%** SIGNIFICANT INCREASE

UNEMPLOYMENT FRAUD

73% OVERALL INCREASE | **41%** SIGNIFICANT INCREASE

FRAUD BY VENDORS AND SELLERS

69% OVERALL INCREASE | **33%** SIGNIFICANT INCREASE

PAYMENT FRAUD

68% OVERALL INCREASE | **31%** SIGNIFICANT INCREASE

IDENTITY THEFT

67% OVERALL INCREASE | **29%** SIGNIFICANT INCREASE

Objectives of IS Audit

- 1. To determine **information and related technological security loopholes** and recommend feasible solution.
- 2. Examining whether **IT processes and IT Resources combine together** to fulfill **intended objectives** to ensure **effectiveness, efficiency , economy, compliance**
- 3. IS auditors **- develop & implement a risk-based IS audit strategy as per IS audit standards, regulatory guidelines** and internal policies
- 4. IS auditors to evaluate **effectiveness of IT governance structure to determine whether IT decisions, directions and performance support entity** 's strategies and objectives.
- 5. IS auditors **evaluate ERM practices to determine - entity's IS-related risks** are properly **managed & secure.**

CONFIDENTIALITY, INTEGRITY, AVAILABILITY

- The CIA triad refers to an information security model made up of the three main components:
  - Confidentiality
  - Integrity and
  - Availability
- ***Confidentiality:*** **often associated with secrecy and use of encryption. Confidentiality in this context means that the data is only available to authorized parties**.
- ***Integrity:*** **Data integrity refers to the certainty that the data is not tampered with or degraded during or after submission. It is the certainty that the data has not been subject to unauthorized modification, either intentional or unintentional**.
- ***Availability:*** This means that the information is available to authorized users when it is needed

Cookies - analysis

- Small data file that is placed on computer or other device **to allow a site to recognize visitor as a user when you return to the Site** using same computer and web browser, either for the duration of your visit (using a 'session cookie') or for repeat visits (a 'persistent cookie').
- **Cookies :**

❑ personalize content and ads, to provide social media features

❑ analyze traffic.

❑ Entities also share information about visitor's use of website site with entities' social media, advertising and analytics partners- **Potential Risk**

- Most browsers automatically accept cookies by default,
- Settings **can be adjusted** as per user preferences.
- If certain cookies disabled, some features of website **may not available** or function properly.

Edit logs

- Logs record every action as it happens
- **Logs** : what an actor (user or entity) did.:
- [timestamp] User A did action Y
- [timestamp] User B did action Z
- [timestamp] User C did action Y
- **A log** is a recording of what happens on a system
- **An audit trail** is a recording of all user actions

Audit trail

- **Audit Trails** : what sequence of actions occurred in order for a certain state to be created.
- connects actions and what other things happened as a result.
- **Example :**
- [timestamp] User A did action Y
- [timestamp] System received Y and did action Z to data store
- [timestamp] Data store was updated with data and sent notification back to User A

Types of IS 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	

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

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.

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.

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.

Network Audits (Vulnerability And Penetration Testing- VAPT)

(a) **Client/Server, Telecom, Intranets, Extranets**: audit to scrutinize that controls are in place on client (computer receiving services) server

(b) **Auditing management and security of networks – IDS, DMZ etc**

(c) **Monitoring extent to which network security aligns with standards**

(d) **Assessment of Vulnerability & Penetration Testing (VAPT) of networks**

(e) **Configuration of various network devices like routers**

(f) Enterprise's **internal network, along with a business's overall network** (including all LAN/WAN, wireless, and Internet access).

(g) constant **scanning, testing & traffic monitoring** of all network operations.

(h) enterprise's **web services** (e.g., web hosting services for website),

IS Audit process flow

1. IS Audit strategy
2. Plan IS Audit
3. Follow internationally accepted standards.
4. planning and the documentation of the work
5. Knowledge of the auditee Organisation
6. Materiality - IS auditor should establish levels of materiality to meet audit objectives
7. IS Audit Programme preparation & documentation
8. IS Audit completion time
9. Resource allocation
10. Project budget
11. Internal Control Evaluation, Risk assessment (SA 315, 330)

Relevant Auditing Standards

- **SA 315:** Identifying and Assessing the Risk of Material Misstatements through Understanding the Entity and its Environment which guides the Identification &Assessment.
- **SA 330:** The Auditor's Response to Assessed Risks elucidates the responses.
- **Conventional Approach :** Get understanding of :

✓ the relevant industry,

✓ legal frameworks,

✓ operations of entity,

✓ governance structure,

✓ financing modes,

✓ selection & application of accounting policies & strategies

IS Audit process

Techniques :

- own observations,
- inspections of process execution,
- walkthrough activities,
- Inquiries with management & staff,
- external clarifications,
- past IS audit reports etc.

•**SA 520 : Analytical Procedures** are then employed to assess the significance, relevance of risks to financial reporting and also the likelihood of their occurrence.

1.1.3. Controls

(a) **Deterrent Controls:** Deterrent Controls are designed to deter unauthorised people, internal as well as external, from accessing the information and information systems.

(b) **Preventive Controls:** Preventive Controls **prevent the cause of exposure** from occurring or **at least minimize the probability** of the occurrence of unlawful events.

(c) **Detective Controls:** When a cause of exposure has occurred, **detective controls report its existence in an effort to arrest further damage** or minimize the extent of damage. **Detective controls limit the losses**, if an unlawful event at all occurs.

(d) **Corrective Controls:** Corrective Controls are designed to help the organization recover from a loss situation. **BCP = corrective control**. Without corrective controls in place, organisation will suffer from risk of loss of business and other losses, **due to its inability to recover essential IT based services**, information after disaster has taken place.

- IS Auditors will require to ascertain that **adequate control exists to cover each likely unlawful event**.
- TOC : If unlawful event is covered by a control, the IS auditors will require to evaluate whether the **control is operating effectively**. If more than one control covers an unlawful event (i.e., redundant controls), the IS auditors will require to verify that all these **controls operate effectively.**

A. IS Preventive Control checklist (Best practices)

1. Security awareness, staff tech training
2. Employ qualified personnel, EBC – Background check
3. Fencing, security guards
4. Lock & key
5. SOD
6. FFE – fire
7. Biometric access controls
8. Anti-virus software
9. Firewalls
10. Digital signature
11. Smart cards / access cards
12. Passwords, PIN,OTP
13. Encryption
14. User registration for access to IPF
15. Restriction to use smart phones (camera), USB drives, CD in critical IPF
16. No smoking, eating in IPF

B. IS Detective Control checklist (Best practices)

1. Motion detectors-
2. Smoke & fire detectors
3. Video surveillance cameras
4. Audit trails
5. CCTV
6. IDS
7. IS Review & audit
8. Mandatory leave / duty rotation
9. Sensors, alarms
10. Performance monitoring
11. Management Review

C. IS Corrective Control checklist (Best practices)

1. Power back up
2. Automatic load restoration after diagnosis of voltage collapses due to load increase
3. BCP
4. Data & software back up
5. DRP
6. Review of ITIL, IS Security Standards

Strategic plan for IT Department

(a) IT departmental **resource allocation**

(b) The strategic utilization of IT in order to optimize internal operations and increase profits

(c) The **skillsets required** in the IT department

(d) Managerial and personnel & departmental teams (e.g., VP of IT, CIO, CTO, R&D, IT security)

(e) Required IT systems of the IT infrastructure

(f) Critical problems that IT department is envisioned to solve – currently and as the company grows

(g) Expectations of stakeholders/investors, along with agreed-upon long-term goals

(h) IT Department Structure (Adaptive and Evolve)

Centralized vs Decentralized IT Structures

- **Centralized Structure**: A centralized IT departmental model is one where all **core IT systems and networks are managed by a central organization,** such that all systems can be easily integrated and managed from a single IT central hub.

(a) **Centralized Structure Pros**: Better Budget control, easier governance, better standardization, better alignment across the entire technology portfolio, easier project/workflow integration, more feasible IT management

(b) **Centralized Structure Cons**: may become bureaucratic, business departments may be unhappy

- fighting with other departments to get their tech initiatives prioritized.

- **Decentralized Structure**: A decentralized IT departmental structure is one where the management of critical IT components, system controls and networks is **distributed amongst multiple, different core IT centers** within the overarching enterprise IT infrastructure, allowing different sub-departments and teams to utilize different resources within their own sub-systems/intranets.

(a) **Decentralized Structure Pros**: Individual departments/business units have **more direct control over their tech projects** and priorities; generally decentralized groups can get faster results (less overhead and prioritization fights).

(b) **Decentralized Structure Cons**: Solutions optimized at the department level **often result in inefficiencies at the enterprise level** ("silos" of disconnected data and business processes);

(c) too much departmental independence can **lead to integration challenges** and unnecessarily duplicative systems and data.

Internal vs Outsourced IT Staff

- Businesses may save over 15 to 20 % in costs by outsourcing specific tasks
- COVID era : cost saving

IT roles that are often outsourced to skilled professionals:

- Support Desk
- Network Administrator
- Software Developer
- Software Tester
- Engineer
- Security Analyst
- Systems/Database Engineer

Dev Ops

DevOps (**Dev+ Ops** : set of practices **combining software development & IT operations**. (**Software Dev & Operations)**

DevOps –

• complementary to ‘’Agile approach’’

•Inspired by –’’The Toyota Way’’

•PDCA Cycle of Lean & Deming

1. Coding – code development and review, source code management tools
2. Building
3. Testing
4. Packaging - application pre-deployment staging.
5. Releasing – change management, release approvals
6. Configuring – infrastructure configuration and management
7. Monitoring – applications performance monitoring

1.2 ITIL- introduction

- **Information Technology Infrastructure Library**
- ITIL - comprehensive framework detailing how **IT department can optimize its services & personnel-communications**, + best practices
- **to better customer experiences and increase bottom line.**
- ITIL framework used to help executives **understand different roles of IT sub-departments**,
- ITIL framework offers **valuable insights that can help strategic planners craft the ideal structure for a company's IT department**.

ITIL Framework

- ITIL framework offers **5 core processes** = align all business goals with IT infrastructure:

1. ***Service Strategy***: Aligning critical business goals/model with the components and services of the enterprise's IT infrastructure
2. ***Service Design***: The IT services that the IT systems offer in order to support the business's operations
3. ***Service Transition***: The transition from a planning/developmental phase to an operational/management phase
4. ***Service Operation***: Operating all services according to SLA in place
5. ***Continual Service Improvement***: Analyzing and offering improvements for each service in order to increase service quality

IT Delivery Models

- Developing **in-house** IT capabilities to complete projects or provide services**: costly & risky**, if IT needs **constantly changing**.
- When companies look **for outside help** in fulfilling IT business needs, they consider 2 delivery models:
- **1. Staff Augmentation** - allows organizations **to add staff to their existing teams based on additional skills required**
- **2. Managed Services-** allows it to free up specialist knowledge within organization & focus on **core business activities**.
- IS Auditors : evaluate, advise management on suitable model

Comparing Managed Services to Staff Augmentation

Managed Services (MSP)	Staff Augmentation
Supplier assumes control of all or part of the execution component of IT.	Supplier commits to providing resources of defined capability at a price.
Service Delivery commitments expressed as "Service Levels".	No service delivery commitments.
Committed Scope and Term which ensures accountability.	Limited commitment.
Costs can be tied to quantifiable results.	Pricing tied to hours worked and availability.
Supplier Managed Delivery Model, processes and tools.	Client manages the delivery model (including individual subcontractors); process and tools.
Knowledge must be transferrable according to a contractual commitment.	Knowledge vested in the individual.
Supplier manages the risks of meeting project deadlines, transition and operations.	All delivery risk remains with Business.

CAAT s

A. Computer Assisted Audit Techniques & Risk Assessment

- The Auditors may choose to use the Auditees CIS itself or employ their own computers as audit tools. The extent to which an auditor uses CAAT's &Manual Techniques would depend on following factors:

(i) Practicality of Manual Testing, given to volume of data

(ii) Cost effectiveness of CAAT's

(iii) Availability of Audit Time & Client's Computers Facility

(iv) Level of Experience & Expertise in using CAAT's

- Extent to which CAAT's are used in Internal Audit functions &How external auditor relies on the same

Audit software

- **Audit Software**: These are the programs designed to carry out **Test of controls & Substantive procedures**, which include:

(a) ***Packaged Programs****:* These are **pre-prepared generalized programs that are not client specific**, used for selection of statistical samples, arithmetical calculations and for checking gaps in processing sequences.

- Eg: Audit Control Language (ACL) & Interactive Data Extraction and Analysis (IDEA).

IDEA - Overview

- **IDEA is Specialised & support Audit techniques / software used for data importing, extraction and analysis.**
  - IDEA
    - CAAT
    - Development
    - Auditing Using Idea
    - Downloading Data
    - Function in IDEA
  - Internet
  - Report

IDEA- Computer Assisted Auditing Technique

- Interactive Data Extraction and Analysis
- A comprehensive CAAT
- Helpful for Auditors, Financial Managers, Investigators and Accountants
- display, analyze, manipulate, sample or extract from data files from almost any source - mainframe to PC, including reports printed to a file
- Lower audit cost, enhance the quality to work and take on new roles by putting the power of IDEA

Audit Command Language (ACL)

- ACL is the market leader in computer-assisted audit technology and is an established forensics tool.

Clientele includes …

- 80 % of the Fortune 500 companies
- over two-thirds of the Global 500
- the Big Four public accounting firms

Audit Command Language

ACL is a computer data extraction and analytical audit tool with audit capabilities …

- Statistics
- Duplicates and Gaps
- Stratify and Classify
- Sampling
- Benford Analysis

Thank You

Arijit Chakraborty