The Institute of Cost Accountants of India

INFORMATION SYSTEM SECURITY AUDIT

BATCH: 5

DISSA
INFORMATION SYSTEM SECURITY AUDIT

Elocutionist: Dr. Saurabh Maheshwari

Chapter - 4

CYBER SECURITY AND CYBER FORENSICS

WHAT IS IS-SECURITY & WHY DO WE NEED IT?

What?

- Information systems security, more commonly referred to as InfoSec, refers to the processes and methodologies involved with keeping information confidential, and available while assuring its integrity.
  It also refers to:
  - Access controls prevent unauthorized personnel from entering or accessing a system.
  - Protecting information no matter where that information is, i.e. in transit (such as in an email) or a storage area.
  - The detection and remediation of security breaches and documenting those events.

Why?

- Reducing the risk of data breaches and attacks in IT systems. Applying security controls to prevent unauthorized access to sensitive information. Preventing disruption of services, e.g., denial-of-service attacks. Protecting IT systems and networks from exploitation by outsiders.

WHAT IS CYBER SECURITY?

Cyber Security

- Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber-attacks.
- It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks, and technologies.

INFORMATION SECURITY MANAGEMENT

- Senior Management Commitment and Support
  - Align IT Risks with Business Objective
  - Proactive Approach
  - Adoption of Standards
  - Framing IS Policies
  - Exception Handling
  - Segregation & Rotation of Duties
  - Training and Awareness Programmes
  - Configuration Management
- Challenges Faced by Management in Implementing IS Security
  - Implementing Policies
  - Computer Crimes & Exposures
  - Incident Handling & Response

ENTERPRISE RISK MANAGEMENT [ERM] FRAMEWORK

1. Assets Identification
2. Assets Valuation and Classification
3. Risk Listing
4. Risk Classification
5. Risk Assessment
6. Risk Ranking / Risk Prioritization / Heat Map
7. Risk Management / Control Adjustment / Risk Treatment / Risk Response
8. Risk Audit / Security Review

… CONTD

1. Assets Identification
2. Assets Valuation and Classification
3. Risk Listing
4. Risk Classification
5. Risk Assessment
6. Risk Ranking / Risk Prioritization / Heat Map
7. Risk Management / Control Adjustment / Risk Treatment / Risk Response
8. Risk Audit / Security Review

- Some Important Information Assets
  - Computers / Workstations / Terminals / Nodes
  - Servers
  - Peripheral Devices
  - Networking / Telecommunication Equipment
  - Data & Database
  - Processes
  - Patents / Trademarks
  - Users
  - Other
- Auditor's Role

… CONTD

1. Assets Identification
2. Assets Valuation and Classification
3. Risk Listing
4. Risk Classification
5. Risk Assessment
6. Risk Ranking / Risk Prioritization / Heat Map
7. Risk Management / Control Adjustment / Risk Treatment / Risk Response
8. Risk Audit / Security Review

- Assets Valuation
- Assets Classification
  - Tangible
    - Computers / Workstations / Terminals / Nodes
    - Servers
    - Peripheral Devices
    - Networking / Telecommunication Equipment
    - Others (Furniture, Electrical Equipment, Building, Users, etc.)
  - Intangible
    - Processes
    - Patents / Trademarks / Intellectual Capital
    - Goodwill
    - Data & Database
    - Others (Documents, Accounts, Internet Domains, Customer Lists, etc.)
- Classification Schemas
- Preparing Information Assets Register (IAR)
- Auditor's Role

… CONTD

1. Assets Identification
2. Assets Valuation and Classification
3. Risk Listing
4. Risk Classification
5. Risk Assessment
6. Risk Ranking / Risk Prioritization / Heat Map
7. Risk Management / Control Adjustment / Risk Treatment / Risk Response
8. Risk Audit / Security Review

- IT risks include hardware and software failure, human error, spam, viruses and malicious attacks, as well as natural disasters such as fires, cyclones or floods.
- The general conclusion from our literature survey is that the IS risk literature is a jumble of diverse risk models and partially overlapping, atheoretical lists of risk factors and risk components.
- With 100’s and 1000’s of risks on Business Information System, listing all possible risk is itself is a tedious and time consuming task.
- Even in listing we have to consider view point of many individuals who have vested interest in the well being of company.

… CONTD

1. Assets Identification
2. Assets Valuation and Classification
3. Risk Listing
4. Risk Classification
5. Risk Assessment
6. Risk Ranking / Risk Prioritization / Heat Map
7. Risk Management / Control Adjustment / Risk Treatment / Risk Response
8. Risk Audit / Security Review

- On the basis of Nature
  1. Physical
  2. Environmental
  3. Administrative
  4. Legal
  5. Logical
- On the basis of Application
  1. Boundary
  2. Input
  3. Process
  4. Output
  5. Storage
- On the basis of Resources
  1. Hardware
  2. Software
  3. Database
  4. Network
  5. Human
- On the basis of Business
  1. Strategic
  2. Market
  3. Financial
  4. Operational
  5. Technical

  and more

… CONTD

1. Assets Identification
2. Assets Valuation and Classification
3. Risk Listing
4. Risk Classification
5. Risk Assessment
6. Risk Ranking / Risk Prioritization / Heat Map
7. Risk Management / Control Adjustment / Risk Treatment / Risk Response
8. Risk Audit / Security Review

On the basis of Nature

1. Physical
2. Environmental
3. Administrative
4. Legal
5. Logical/Cyber

- Risks
- Reason
- Impact
- Policy & Controls
- Auditor's Role

… CONTD

1. Assets Identification
2. Assets Valuation and Classification
3. Risk Listing
4. Risk Classification
5. Risk Assessment
6. Risk Ranking / Risk Prioritization / Heat Map
7. Risk Management / Control Adjustment / Risk Treatment / Risk Response
8. Risk Audit / Security Review

On the basis of Application

1. Boundary
2. Input
3. Process
4. Output
5. Storage

- Risks
- Reason
- Impact
- Policy & Controls
- Auditor's Role

… CONTD

1. Assets Identification
2. Assets Valuation and Classification
3. Risk Listing
4. Risk Classification
5. Risk Assessment
6. Risk Ranking / Risk Prioritization / Heat Map
7. Risk Management / Control Adjustment / Risk Treatment / Risk Response
8. Risk Audit / Security Review

On the basis of Resources

1. Hardware / Devices
2. Software
3. Database
4. Network
5. Human

- Risks
- Reason
- Impact
- Policy & Controls
- Auditor's Role

… CONTD

1. Assets Identification
2. Assets Valuation and Classification
3. Risk Listing
4. Risk Classification
5. Risk Assessment
6. Risk Ranking / Risk Prioritization / Heat Map
7. Risk Management / Control Adjustment / Risk Treatment / Risk Response
8. Risk Audit / Security Review

On the basis of Business

1. Strategic
2. Market
3. Financial
4. Operational
5. Technical
6. Audit
7. Logistic

and more

- Risks
- Reason
- Impact
- Policy & Controls
- Auditor's Role

… CONTD

1. Assets Identification
2. Assets Valuation and Classification
3. Risk Listing
4. Risk Classification
5. Risk Assessment
6. Risk Ranking / Risk Prioritization / Heat Map
7. Risk Management / Control Adjustment / Risk Treatment / Risk Response
8. Risk Audit / Security Review

- Methods of Risk Assessment
  - Qualitative
  - Quantitative
- Parameters to consider for Risk Assessment
  - Vulnerability Assessment
  - Probability / Likelihood Assessment
  - Exposure Analysis
  - Impact / Business Impact Analysis

… CONTD

1. Assets Identification
2. Assets Valuation and Classification
3. Risk Listing
4. Risk Classification
5. Risk Assessment
6. Risk Ranking / Risk Prioritization / Heat Map
7. Risk Management / Control Adjustment / Risk Treatment / Risk Response
8. Risk Audit / Security Review

- After ‘Risk Assessment’ is done in a systematic manner, the organization must be able to list the risk in such a manner so that high priority, risks are treated or handled first. Also known as Risk Matrix in some frameworks.
- Risk ranking can also be done through the “Heat Map” process.

Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

… CONTD

1. Assets Identification
2. Assets Valuation and Classification
3. Risk Listing
4. Risk Classification
5. Risk Assessment
6. Risk Ranking / Risk Prioritization / Heat Map
7. Risk Management / Control Adjustment / Risk Treatment / Risk Response
8. Risk Audit / Security Review

- Risk Aggregation: It relates to the process of summing and showing the interaction between single or individual risks, to see the bigger picture.
- Risk Scenarios: The risk scenario is chosen by reviewing the potential incidents that could occur within a situation and selecting one at a time for consideration during the assessment.
- Risk Turndown: Turn down is a situation where an individual has determined a risk cannot be undertaken or considered on the organization as given.
- Risk Avoidance: Not performing any activity that may carry risk. A risk avoidance methodology attempts to almost nullify the vulnerabilities which can pose a threat.
- Risk Mitigation: Risk mitigation can be defined as taking steps to reduce adverse effects. Risk avoidance and mitigation can be achieved through policy and procedure, training and education, and technology implementations.
- Risk Transfer / Risk Sharing: Risk transfer is a risk management and control strategy that involves the contractual shifting of a pure risk from one party to another. One example is the purchase of an insurance policy.
- Risk Tolerance / Risk Acceptance: This is the level of risk that an organization can accept per individual risk.
- Risk Appetite: Risk appetite is the total risk that the organization can bear in a given risk profile, usually expressed in aggregate.

… CONTD

1. Assets Identification
2. Assets Valuation and Classification
3. Risk Listing
4. Risk Classification
5. Risk Assessment
6. Risk Ranking / Risk Prioritization / Heat Map
7. Risk Management / Control Adjustment / Risk Treatment / Risk Response
8. Risk Audit / Security Review

- After all risks are treated as per policy and resources available in the best possible manner by an organization, a very important document called “Risk Register” is prepared.
- A risk register is a document used as a risk management tool and to fulfill regulatory compliance acting as a repository for all risks identified and includes additional information about each risk, e.g. nature of the risk, reference and owner, mitigation measures.
- A regularly and properly maintained Risk Register will help in ‘Risk Profiling’ and can also act as a proactive tool in finding which risk can occur, at what intensity, can cause what damage and what preventive measures can be taken to manage it.

… CONTD

1. Assets Identification
2. Assets Valuation and Classification
3. Risk Listing
4. Risk Classification
5. Risk Assessment
6. Risk Ranking / Risk Prioritization / Heat Map
7. Risk Management / Control Adjustment / Risk Treatment / Risk Response
8. Risk Audit / Security Review

- Before understanding Risk Audit you must go through the concept of Acceptable risk. The risk exposure that is deemed acceptable to an individual, organization, community or nation. Acceptable risks are defined in terms of the probability and impact of a particular risk after considering the vulnerabilities. In practice, risk often can't be reduced to zero due to factors such as cost and secondary risk.
- When a Risk Audit or Security review is done, tools used by hacker / attacker are used and a Penetration Testing (also known as Pen Test) is done with the intention of assessing the efficacy of the controls implemented to safeguard the system.
- Any risk which was left out (due to any reason) and remaining risk coming out of this Pen Test is known as “Residual Risk”.
- This residual risk must be under acceptance level to keep things going else IS Auditor has to put more efforts to put more controls at high risk / left out areas to keep risk under acceptable level.

COMMON CYBER ATTACKS

1. Backdoor
2. Blue Jacking
3. Buffer Overflow
4. Cyber Stalking
5. Cyber Terrorism
6. Cyberwarfare
7. Data Diddling
8. Denial of Service & DDoS
9. DNS Spoofing
10. Email Spoofing
11. Identity Theft
12. Keystroke Logger
13. Bombs
14. Piggybacking
15. Salami Theft
16. Sensitive Data Exposure
17. Injection
18. Trojan
19. Virus
20. Worms
21. Website Defacement
22. Social Engineering
23. Vishing
24. Phishing
25. IoT attaches
26. Botnet
27. Brute Force
28. Spoofing Attacks
29. Reconnaissance
30. Injections
31. Ransomware
32. Ad Hoc Networks
33. Deepfake
34. Juice Jacking

… and many more

Two-thirds of the Earth is covered with Water and the rest one-third is covered with Auditors from different verticals evaluating the business operations from different angles.

- Dr. Saurabh Maheshwari

THANKS!

Any questions?

PHYSICAL RISKS AND CONTROLS

Risks

- Unauthorized person gaining access
- Damage Vandalism or theft of resources
- Data theft
- Embezzlement of computer supplies
- Public disclosure of sensitive information.

Reasons

- Current or former staff misusing access rights
- Rivals / Organized criminals / Ignorant
- People under financial or emotional problems
- Outsources agencies
- Employees under termination notice

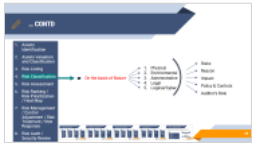
Impact

- Confidentiality, and privacy breach
- Demand of ransom
- Assets loss
- Goodwill loss
- Misuse of data
- Crushed stakeholder's trust

Policy & Controls

- Physical security policy
- Maintaining Logs
- Locks
- CCTV
- Perimeter fencing
- Identification badges
- Many more …

Auditor's Role ?



ENVIRONMENTAL RISKS AND CONTROLS

Risks

- Fire bust
- Water flow
- Power issues
- Earthquake
- Tornado
- Tsunami, Cyclones
- Major temperature variations
- War
- Pandemic
- Insects (Rats, Termites, Fungi)

Reasons

- Every risk has their own reasons
- Sometime they may be natural unavoidable issues and
- Sometime man made

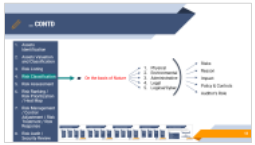
Impact

- Confidentiality, and privacy breach
- Assets loss
- Work loss
- Data loss
- Life loss

Policy & Controls

- Environmental security policy
- Controls to be discussed during session

Auditor's Role ?



ADMINISTRATIVE RISKS AND CONTROLS

Risks

- No policies
- Outdated policies
- Open exception
- Open bypass procedures

Reasons

- Loopholes from top authorities in drafting and implementing policies and procedures
- Lethargic attitude towards framing code of conduct

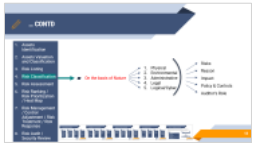
Impact

- Confidentiality, and privacy breach
- Assets loss
- Work loss
- Data loss
- IP loss
- Crushed stakeholder's trust

Policy & Controls

- Properly drafted policies for everything
- Regularly updating policies
- Implementation of Policies
- Creation and review of log file.

Auditor's Role ?



LEGAL RISKS AND CONTROLS

Risks

- Compliance risk
- Reputational risk
- Dispute risk
- Contractual risk

- Reference: https://blog.ipleaders.in/legal-risks/

Reasons

- Neglecting legal framework
- Bypassing laws for personal or organizational benefits

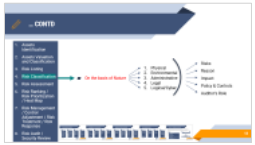
Impact

- Fine
- Imprisonment
- Paneities
- Sanctions
- Legal proceeding

Policy & Controls

- Legal policy
- Knowledge of prevailing laws
- Abiding all applicable laws
- Updating system to incorporate all legal changes

Auditor's Role ?



LOGICAL / CYBER RISKS AND CONTROLS

Logical threats are those that may damage your software systems, data, or network without actually damaging your hardware. These are actually a major concern and are unique when you are working on any Information System.

There are lot many logical threats and are ever increasing, so for understanding it better lets classify them in some heads to understand better.

Logical Risks

1. Logical Access Issues
2. Malicious Codes
3. Data Leakage
4. Flow of Unwanted Data
5. Intruders / Hackers
6. Impersonation
7. Denial of Services / Distributed Denial of Services
8. SQL Injection
9. Website Defacement
10. Social Engineering and many more …

Reasons & Impacts

Known to all

Policies & Controls

To be discussed in detail during the session

Auditor's Role ?

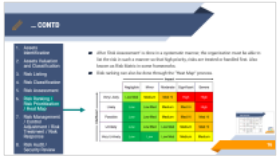
MAJOR CYBER ISSUES - 2025

- Malware
- Phishing / Spear Phishing
- Spoofing
- Social Engineering
- Blue Jacking
- Ransomware
- Data Breach
- IoT / IoMT Attacks
- Reconnaissance
- DoS / DDoS Attacks
- DNS Attacks
- Network Sniffing
- Brute Force Attack
- Crypto Jacking
- Insider Attacks
- Juice Jacking
- Advanced Persistent Threat
- Web Session Cookie Issue
- Business Invoice Fraud
- Cloud Access Management
- Third Party Vulnerabilities
- Privileged User Compromise
- Deepfake
- Digital Arrest

... and many more

SAMPLE RISK MATRIX

Asset	Threat	Vulnerability	Impact	Likelihood	Risk	Control Recommendations
Servers Critical	System failure — Overheating in server room High	Air-conditioning systems is ten years old. High	All services (website, email, etc.) will be unavailable for at least 3 hours. Critical	High Current temperature in server room is 40C	High Potential loss of $50,000 per occurrence	Buy a new air conditioner, $3,000 cost.
Website Critical	Malicious human (interference) — DDOS attack. High	Firewall is configured properly and has good DDOS mitigation. Low	Website resources will be unavailable. Critical	Medium DDOS was discovered once in 2 years.	Medium Potential loss of $10,000 per hour of downtime	Monitor the firewall.
Servers. Critical	Natural disasters — Flooding High	Server room is on the 3rd floor. Low	All services will be unavailable. Critical	Low Last flood in the area happened 10 years ago.	Low	No action needed.
Files on a file share Medium	Accidental human interference — Accidental file deletions High	Permissions are configured properly; IT auditing software is in place; backups are taken regularly. Low	Critical data could be lost but almost certainly could be restored from backup. Low	Medium	Low	Continue monitoring permissions changes, privileged users and backups.



RISK ON RESOURCES

HARDWARE & DEVICES	SOFTWARE	DATABASE	HUMAN RESOURCE	NETWORK
• Physical damage • Mishandling • Theft • Damage due to environmental disturbances • Technical flaws • Compatibility issues • Intentional mis-configuration	• Bugs & malicious codes • Piracy issues • Compatibility issues • Mishandling • Disgruntled users • Hackers • Improper application controls • Access issues	• Leakage • Tampering • Mishandling • Unavailability • Wrong data • Access issues • Size of data • Format of data • Dumping of data	• Life danger • Ethical problems (theft and embezzlement) • Employee unrest • Fatigue problems • Competency issues	• Misconfiguration • Data leakage • Hacking • Protocol flaws • Access issues • Compatibility issues • Many more already discussed

Controls and Auditor's Role will be discussed during session.