Domain 1: Security and Risk Management

Index

CIA Triad:

a. Confidentiality (C): Resources should be protected from unauthorized access
b. Integrity (I): Resources should be protected from unauthorized modification
c. Availability (A): Resource should be accessible to authorized parties

IAAA:

a. Identification: Action owner identifies themselves
b. Authentication: Action owner proves their identity
c. Authorization: The action owner is allowed/disallowed to perform an action
d. Auditing: The action owner's actions are logged

Accounting:

The action owner logs are reviewed for violations

Non-repudiation:

The action owner cannot deny his/her actions

Governance(Not us):

- Decided by C - level(CISO, CFO, etc.) executives
- Sets direction for the organization on the basis of prioritization and decision-making
- Monitors performance and compliance
- Decides risk appetite

Management(Us):

- Plans to implement directions on governance
- Minimize risk to the tolerance level

Principle:

There are 2 types of principles:

A. Top Down:
    a. Works on the directions given by upper management.
    b. Everything is done with the support of upper management
    c. Good for the security implementation
B. Bottom Up:
    a. Works on the demands and requests given by staff
    b. Bad for security.

Standards and Frameworks

There are many security frameworks and standards available for security implementation and guidance for any organization. A few examples are

a. PCI DSS: Mostly used for financial organizations that hold payment card-related details.
b. COBIT
c. ITIL
d. ISO 27001
    i. This is given by the International Organisation of Standards(ISO) for Information Security Management Systems (ISMS).
    ii. Follows a risk-based approach.
    iii. Monitors using PDCA cycle.
        1. Plan
        2. Do
        3. Check
        4. Act
e. ISO 27002: Focuses on the implementation of ISO 27001.
f. ISO 27005: Risk management
g. ISO 27799: Protection of Personal Health Information (PHI)

Protection Methods

1. Defense in Depth
    a. Multiple layers of security
    b. Includes physical, administrative, and logical controls
        i. Physical: Guards, fence, CCTV
        ii. Administrative: Policies and Procedures
        iii. Logical: Firewall, IDPS
    c. Improves CIA
2. Encryption: Makes data unreadable to unauthorized subjects
3. Data Hiding: Hides data for unauthorized users

Security Governance Principles

Types of Plan:

a. Strategic Plan
   i. 3 to 5 years
   ii. Decide by Governance
   iii. Plans mission, vision, and goals
b. Tactical Plan
   i. 1 year
   ii. Project Management, Hiring, etc.
c. Operational Plan
   i. Few months
   ii. Comprise of methods to achieve the tactical plan

Laws

There are various types of laws:

a. Criminal Law
   i. Violation of criminal law.
   ii. Evidence should be “Beyond a reasonable doubt”
   iii. Punishment may be in the form of fines, jail or both.
b. Civil Law
   i. Contract Disputes between entities
c. Administrative Law
   i. Laws by government agencies

Regulations

a. Computer Fraud and Abuse Act 1986 (CFAA)

Due Care

Mostly a plan to be comply with all applicable regulations and also look if there is any failure to comply any regulation

Due Diligence

It is the effort to maintain the due care. It can include VAPT, security reviews and audits, etc.

Intellectual Property

Copyright

It is mostly for the protection of art or software. It prevents copying the original softwares. It is indicated by © symbol.

Trademark

It is usually logos, names, etc. indicated by ™ symbol if not registered and indicated by ® symbol if registered.

✓ Nike
↙ ↘
Trade Mark Copyright

Patent

It is used to protect inventions. For eg: Medicines

Trade Secrets

These are the organization’s trade secrets which helps in succeeding them. For eg: A special recipe

Import/Export Restrictions

Third Party Security

a. Service Level Agreement (SLA): Agreement to provide certain level of service
b. Right to penetration test and audit

Vendor, Consultants, Contractors, Outsourcing and Offshoring

They should at least follow organization security methods.

Acquisitions

One organization has acquired another organization

Divestiture

The organization is split up.

Security Documents

- a. Policy
  - i. Mandatory
  - ii. High level - Not specific to technology
  - iii. Comprise of regulatory, advisory and informational points
- b. Standards
  - i. Mandatory
  - ii. Specific use of technology
- c. Guidelines
  - i. Non mandatory
  - ii. Usually contains recommendation on how to implement
- d. Procedures
  - i. Mandatory
  - ii. Low level
  - iii. Step by step methods to implement
- e. Baseline
  - i. Mandatory
  - ii. Minimum acceptable requirement

User Security

Personnel/user security is basically securing employees. This can be achieved by:

- a. Awareness
- b. Training
- c. Hiring
  - i. Background checks
  - ii. Non Disclosure Agreement
- d. Termination
  - i. Lock the account, never delete.

Access Control

Categories:

- a. Administrative
  - i. Policies and procedures
  - ii. Regulations
  - iii. Training
- b. Technical
  - i. Hardware, software and firmware
  - ii. Encryption
- c. Physical
  - i. Locks, fences, etc.
  - ii. Guard, Dogs, etc.

Types:

1. a. Preventive: Least Privilege, IPS, firewall
   b. Detective: IDS, CCTV
   c. Corrective: Antivirus, Patching
   d. Recovery: DR, Backup
   e. Deterrent: Fence, Guards
   f. Compensating

Risk Management

Risk = Threat * Vulnerability

Steps:

- a. Identification
  - i. Asset
    - 1. Tangible: Physical Hardware, Anything you can touch
    - 2. Intangible: Data, trade secrets, etc.
  - ii. Team
  - iii. Scoping
  - iv. Tools
  - v. Methods
  - vi. Risk Appetite
- b. Assessment
  - i. Quantitative
  - ii. Qualitative
  - iii. Cost Benefit Analysis
  - iv. Mitigation/Transfer/Acceptance/Avoidance
  - **v. Risk rejection is not acceptable**

    Total Risk = Threat * Vulnerability*Asset Value

Qualitative Risk Assessment

Risk Matrix

		Consequence				
		Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
LIKELIHOOD	**Almost Certain**	H	H	C	C	C
	Likely	M	H	H	C	C
	Possible	L	M	H	H	C
	Unlikely	L	L	M	H	C
	Rare	L	L	M	H	H

Quantitative Risk

Risk registers can be used to monitor the risk.

Risk Analysis

Single Loss Expectancy(SLE) = Asset Value(AV) * Exposure Factor(EF)
Annual Loss Expectancy(ALE) = Annual Rate of Occurrence (ARO) * Single Loss Expectancy(SLE)

Key Goal Indicators (KGI)

Defines a measure that tells management whether a goal has been achieved.

Key Performance Indicators (KPI)

Define actions that determine how well the processes are performing to reach the goal.

Key Risk Indicators (KRI)

Metrics that determine the risk organization is facing.

Risk response and mitigation

a. Mitigation
b. Transfer
c. Acceptance
d. Avoidance

Update risk registers with mitigations to get the risk to an acceptable level.

Business Continuity Planning

Comprise of:

- Continuity of operations plan
- Crisis communication plan
- Critical infrastructure protection plan
- Cyber incident response
- Disaster Recovery Plan
- Information system contingency plan
- Occupant emergency plan

The NIST 800-34 can be followed as the standard.

Explain benefits of BCP

- Cost of disaster
- Regulatory requirements
- Legal consequences
- Loss of customer trust

Business Impact Analysis

Identify critical and non critical assets
Recovery Point Objective (RPO) - Maximum amount of data the organization can tolerate losing.
Maximum Tolerable Downtime (MTD) - Amount of time mission/business process can be disrupted without causing significant harm.
Recovery Time Objective (RTO) - Maximum length of time it should take to restore normal operations following an outage or data loss.
Work Recovery Time (WRT) - Time required to configure a recovered system.

MTD >= RTO + WRT

Mean Time Between Failures (MTBF) - How long will a new/repaired asset function.
Mean Time To Repair (MTTR) - How long it takes to recover a failed system.
Minimum Operating Requirement (MOR) - Minimum requirement for our critical system to function.

Threat Intelligence

Set of activities that an organization undertakes to educate itself about changes in the cyber security threat landscape, and adapt security controls based upon threat information.
Mostly available on Open Source platforms.

Approaches:

- Focused on Assets - Protect valuable assets
- Focused on Attackers - Protect the things that attackers want to attack
- Focused on Software - Protect the software

Threat Hunting

Approach to seek Indicators of Compromise (IOC) on network.
IOC can be of various types:

- Unused file, processes
- Log entries
- Unapproved actions

STRIDE

- Spoofing - Falsifying information to gain access
- Tampering - Making unauthorized changes
- Repudiation - Denying having done an action
- Information Disclosure - Revelation of controlled information
- Denial-of-Service - Prevents the use of an asset
- Escalation of Privilege - Elevates capability of under privileged account

Supply Chain Risk Management (SCRM)

Vendors should perform security activities as organizations follow in their environment.
Phases:

1. Vendor Selection - Request for Proposal (RFP)
2. Onboarding - Verification of contracts
3. Monitoring - Ensure security is followed.
4. Offboarding - Data disposal

Agreements

- Non Disclosure Agreement (NDA)
- Service Level Requirements (SLR)
- Service Level Agreements (SLA) - Penalties
- Memorandum of Understanding (MOU)
- Business Partnership Agreement (BPA)
- Statement of Work (SOW)

Audits and Assessments

- Scope
- Internal Auditors - Reports to executives
- External Auditor
- Gap Analysis

Cloud Audits

SOC Reports

SOC #	**Type 1**	**Type 2**
SOC 1 - Financial	Description	Results of auditor
SOC 2 - Detailed security		
SOC 3 - High level security		