CISSP

Aitizaz Uddin Syed (M.Engg, CISSP, CISSP-ISSAP, CCSP, CRISC, GICSP, TOGAF)

Domain 1
Security and Risk Management

CHAPTER 2
Personnel Security and Risk Management Concepts

Personnel Security Policies and Procedures

- Human is weakest element
- Training vs Awareness
- Job description map responsibilities to duties and tasks & these dictate rights and privileges
- Screen and hiring process based on sensitivity of the role
  - Capability, personality, history, and background

On boarding: Employment Agreements

- On boarding process
- Policy driven hiring
- Sign Documents, NDA, NCA, AUP, Privacy Rules
- Orientation and Socialization
- Identity Access Management (IAM)
- Employee Oversight

-Make reading cybersecurity policies procedures part of orientation and briefing
-Clear sentiments of org attitude towards cyber security
-Time to time review and audit job description, work task, privileges and roles
-Avoid **privilege creep** and monitor for disgruntled employee actions

Some terms related to employee entitlement (Briefly covered in Domain 5)

- Principle of Least Privilege
- Separation of Duties
- Mandatory Vacation
- Job rotation and cross training
- 2 mans control
- Collusion
- Perform UBA and UEBA monitoring
- Special focus on privilege accounts (Privilege Access Management)

Off boarding, Transfers, and Termination Processes

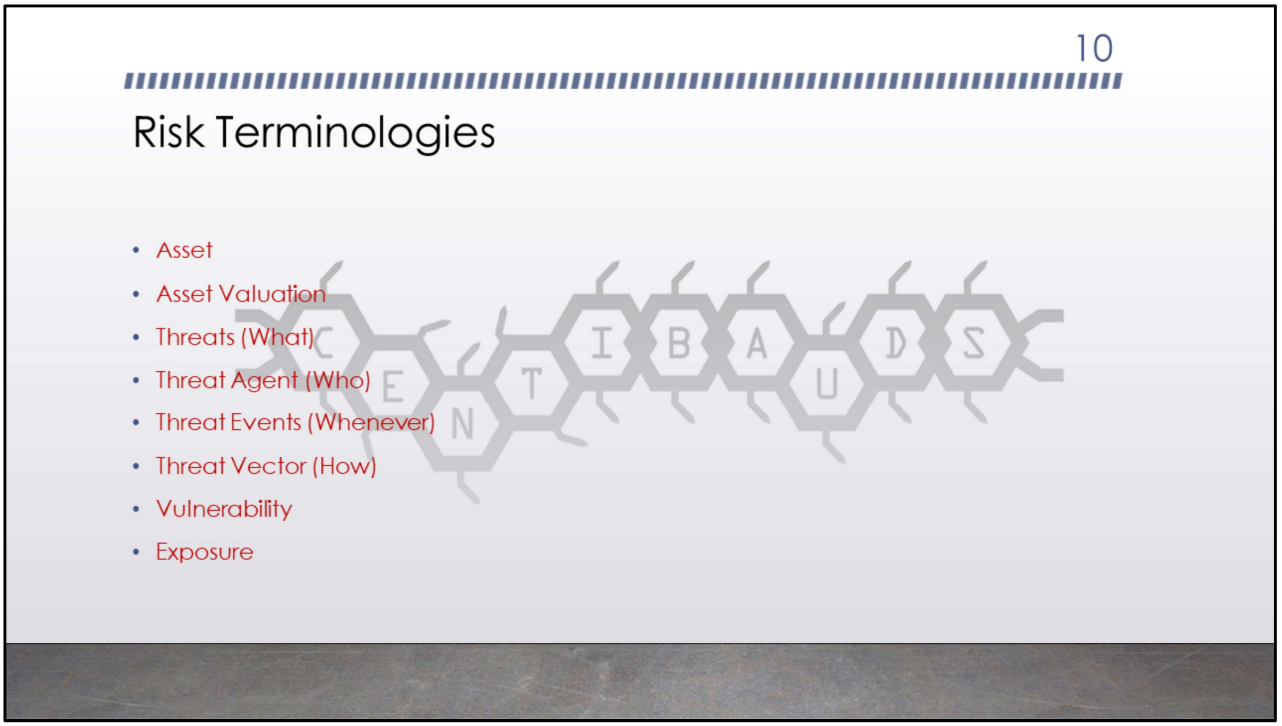
- IAM removal
- In case transfer, removal of existing roles and perform rehiring process to remove old privileges
- Disabling and/or deleting the user account, revoking certificates, cancelling access codes, and terminating other entitlements and privileges
- Deactivate first followed by delete after few months
- Termination in a meeting during which all accesses are revoked and collect all belongings
- Follow professional demeanor escorting by security guards outside to avoid possible confrontation
- Exit interview to learn

Vendor, Consultant, and Contractor Agreements and Controls

- Same as discussed earlier the terms of SLAs, SLRs, MoUs
- Out sourcing benefits and challenges
- Vendor Management System (VMS) track vendors contracts obligations, software coverages and licenses etc..

What is Risk?

- Layman terms: "Something is going to happen with bad consequence and unable to evaluate its repercussion"
- Technical term: "A likelihood that a threat actor successfully exploit a vulnerability in an asset causing an unwanted impact"
- Cybersecurity industry revolves around risk based approach



-Threats : The actions
-Threat Agent: The Actor Intentionally exploit vulnerability
-Threat Vector: The path to inflict threat event
-Vulnerability: Weakness or lack of security control control or safeguard
-Exposure: Susceptible to an event that may cause loss to an asset

Example 1: A cloud based ITMS system (Asset) monthly subscription (Asset Valuation) becomes inaccessible (Threat) as the ISP (Threat Agent) connecting Cloud disconnects (Threat Event) due to router malfunction (Threat Vector). The known glitch in router leading to a malfunctioning is (Vulnerability)

Example 2: A database (Asset) carrying customers sensitive data (Asset Valuation) gets exposed/hacked (Threat) by hackers (Threat Agents) by exploiting SQL injection (Threat Vector) by inserting unwanted meta-characters (Vulnerability) on 23rd April (Threat Event)

Example 3: A datacentre (Asset) carrying servers and applications of south region (Asset Valuation) catches fire (Threat) by electrical spark (Threat Vector) due to failure of a fuse (Threat Agent) after 2 years of its lifetime (Vulnerability)

Risk Terminologies (contd..)

- Risk = [Threat X Vulnerability] model
- Risk = [Consequences X Cause] model

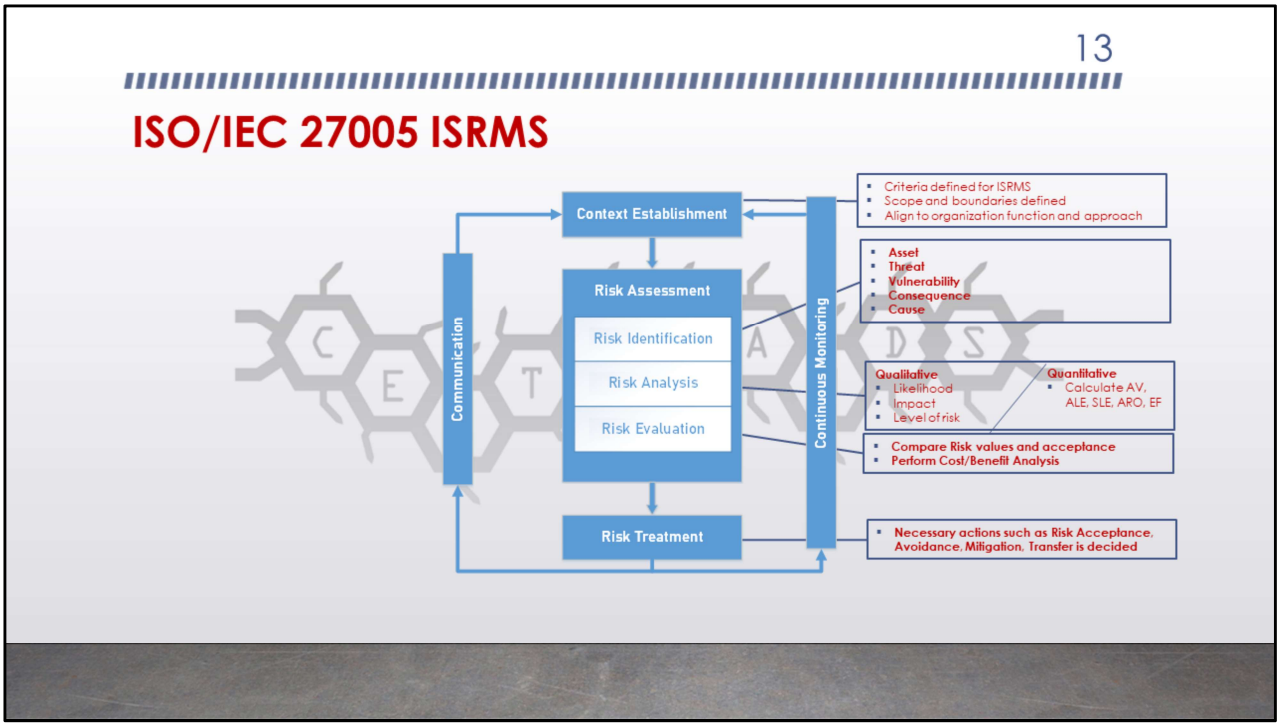
- Risk= Probability of harm vs Impact of harm
- Safeguard : Lessen Threat or Likelihood or Vulnerability
- Attack : Intentional Exploitation of a Vulnerability
- Breach : Intrusion or infiltrate by bypassing or defeating security control (safeguard)
- Hazard : A situation that can cause harm to an asset

-Safeguard reduces threats but not threat actors

Risk Terminologies (contd..)

- **Risk can never be brought to Zero**
- Risk has two components
  - Risk Assessment/Analysis
  - Risk Treatment

Risk = Threat X Vulnerability

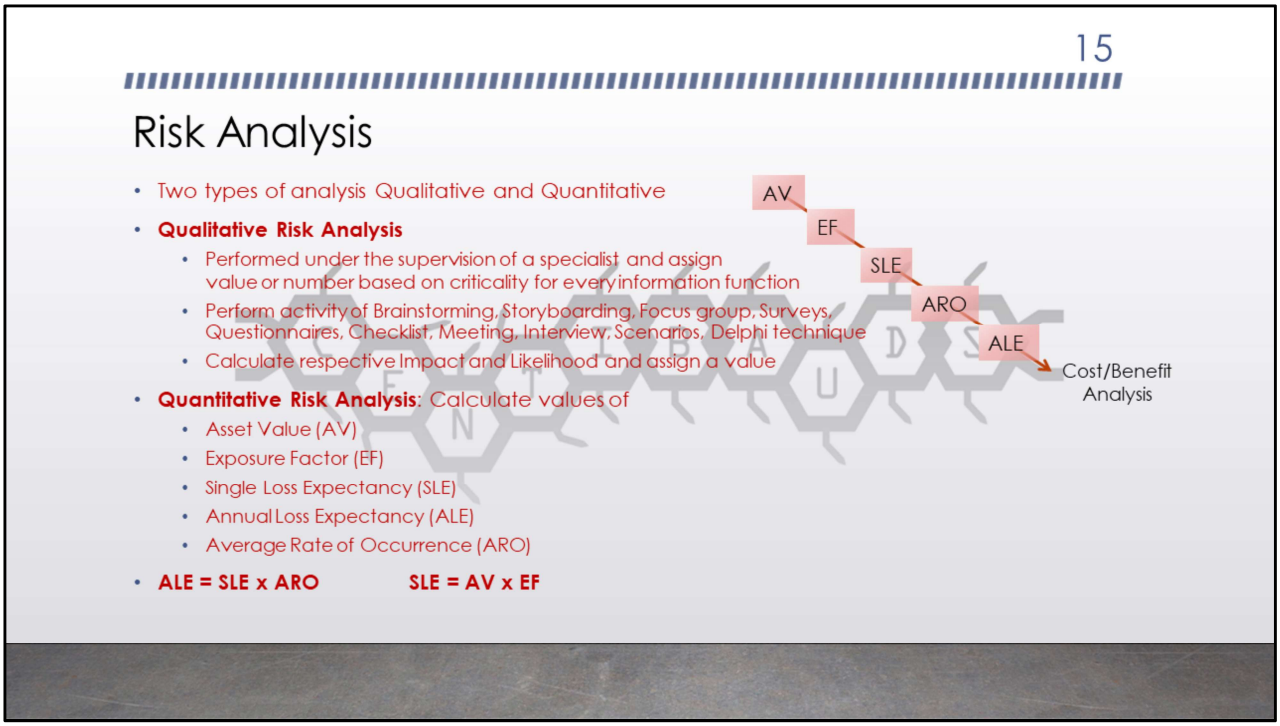


-ISO/IEC provides a guidelines to develop a Risk Management Process for Information Security.

-Risk Assessment has 3 stages : Risk Identification -> Risk Analysis -> Risk Evaluation

Asset Valuation

- Assets are Tangible/Intangible
- Various aspects of it are considered for asset valuation
- Briefly covered in Domain 2



Do some examples here

Consider a house in a dry, wooded area. Wildfire is a (threat) regardless of the building material used to construct the house (i.e., wood or brick). The (likelihood) of a wildfire starting in the wooded area during the summer is more probable than during the winter (threat event). This is also distinct from the (likelihood) of the house burning down (loss event). For the second instance we take into consideration the building material. A wooden house (vulnerable) to fire (threat actor); a brick house is not. For the same threat (a fire starting), the likelihood of impact is, therefore, different depending on the vulnerability.

Next, the destruction of the house is a potential consequence. If the house is occupied, the impact is temporary homelessness for those who live there, which imposes the immediate costs of temporary lodging and a replacement wardrobe. Under those circumstances, it makes sense to take precautions sufficient to address this impact, such as insuring the home against fire or putting in a fire-suppression system, but it is not reasonable to hire a full-time fire crew to watch the house on a daily basis because the cost of the fire crew would exceed the cost of the impact. However, if the house were uninhabited and condemned, the consequences would

have no negative impact, and no precautions may be necessary.

Reference: CRISC Official Manual

16

Risk Evaluation

- Risk Evaluation in Qualitative and Quantitative
  - Risk Response Strategy
  - Risk Appetite
  - Risk Tolerance
  - Risk Limit (in between appetite and tolerance)
  - Consideration of results of Cost/Benefit Analysis in Quantitative

Risk Matrix

Probability \ Impact	H	M	L
H	HH	HM	HL
M	MH	MM	ML
L	LH	LM	LL

- Total Risk = Threat x Vulnerability x Asset value
- Residual Risk = Total Risk- Control Gap(Risk reduced)
- Benefit of a safeguard= [Pre-safeguard ALE - Post-safeguard ALE] - Annual cost of safeguard(ACS)
- Cost of safeguard < Asset Value
- Residual Risk < Risk Appetite

Total Risk (Residual) = (Threat x Vulnerability x Impact) / Countermeasures

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

Risk Treatment

- Mitigation or reduction
- Assignment or Transfer (Insurance)
- Avoidance
- Acceptance
- Reject or ignore

Quantitative Risk Analysis Practice

- Use the following scenario to answer. A small remote office for a company is valued at $800,000. It is estimated, based on historical data, that a fire is likely to occur once every ten years at a facility in this area. It is estimated that such a fire would destroy 60 percent of the facility under the current circumstances and with the current detective and preventative controls in place.
- What is the single loss expectancy (SLE) for the facility suffering from a fire?

A. $80,000 B. $480,000 C. $320,000 D. 60%

- What is the annualized rate of occurrence (ARO)?

A. 1 B. 10 C. .1 D. .01

- What is the annualized loss expectancy (ALE)?

A. $480,000 B. $32,000 C. $48,000 D. .6

Quantitative Risk Analysis Practice (Contd..)

- After implementing security awareness training worth $20K to reduce phishing risks estimated to be ALE of $500K (50 phishing incidents/year), a company still experiences occasional successful phishing attacks worth $50K (5 incidents/year)
- Total Risk in this case is valued at (prior implementation of control):
  A. $20K B. $500K C. $50K D. $520K
- Residual Risk in this case is valued at:
  A. $20K B. $500K C. $50K D. $70K
- The value of Residual risk is compared to which value to determine its acceptance:
  A. Risk Tolerance B. Risk Appetite C. Risk Limit D. Risk Target

The estimated benefit value of security awareness training control to organization is:
A. $450K B. $350K C. $430K D. $70K

-Total Risk = Threat x Vulnerability x Asset value
-Total Risk (Residual) = (Threat x Vulnerability x Impact) / Countermeasures
-Benefit of a safeguard= [Pre-safeguard ALE - Post-safeguard ALE] - Annual cost of safeguard(ACS)

Quantitative Risk Analysis Practice (contd..)

- Use the following scenario to answer. A company has an e-commerce website that carries out 60 percent of its annual revenue. Under the current circumstances, the annualized loss expectancy for a website against the threat of attack is $92,000. After implementing a new application-layer firewall, the new annualized loss expectancy would be $30,000. The firewall costs $65,000 per year to implement and maintain. How much does the firewall save the company in loss expenses?

A. $62,000 B. $3,000 C. $65,000 D. $30,000

- What is the benefit value of the firewall to the company annually?

A. $62,000 B. $3,000 C. –$62,000 D. –$3,000

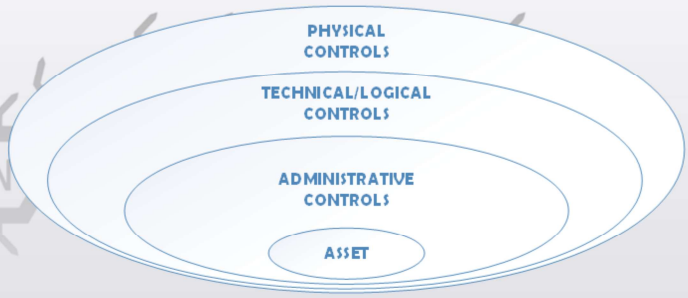
- Which of the following describes the company's approach to risk management?

A. Risk transference B. Risk avoidance C. Risk acceptance D. Risk mitigation

Benefit of a safeguard= [Pre-safeguard ALE - Post-safeguard ALE] - Annual cost of safeguard(ACS)

Types of Controls

- Preventive
- Corrective
- Detective
- Recovery
- Deterrent
- Directive
- Compensating



Types of Controls Practice

- A server that houses sensitive data has been stored in an unlocked room for the last few years at Company A. The door to the room has a sign on the door that reads "Room 1." This sign was placed on the door with the hope that people would not look for important servers in this room. Realizing this is not optimum security, the company has decided to install a reinforced lock and server cage for the server and remove the sign. The company has also hardened the server's configuration and employed strict operating system access controls.
- The fact that the server has been in an unlocked room marked "Room 1" for the last few years means the company was practicing which of the following?

A. Logical security B. Risk management C. Risk transference D. Security through obscurity

- The new reinforced lock and cage serve as which of the following?

A. Logical controls B. Physical controls C. Administrative controls D. Compensating controls

- The operating system access controls comprise which of the following?

A. Logical controls B. Physical control C. Administrative controls D. Compensating controls

Types of Cyber Security Insurance

- Coverage for data breaches
- Financial loss protection
- Legal liabilities
- Reputation management
- Business interruption
- Ransomware protection
- Forensic services
- Incident response
- Regulatory compliance
- Third-party liability

Risk Reporting and Documentation

- Security Control Assessment (SCA) (Checks effectiveness of controls)
- Continuous monitor and measure
- Internal reporting
- Key Risk indicator
- Risk register OR Risk log
- Risk matrix OR Risk Heat Map same to the one displayed in chapter 1
- Risk Assessment is a continuous cycle
- Organization Risk capability is evaluated based on CMM or its form RMM
  - Initial -> Repeatable -> Defined -> Managed -> Optimized

Risk Matrix

Probability			
H	HH	HM	HL
M	MH	MM	ML
L	LH	LM	LL
	H	M	L

Impact

Legacy Devices Risk and Outsourcing

- End of Life (EoL): No more production and updates. Support is there
- End of Service Life (EoSL): No more production, No more support, No more updates
- Outsourcing and 3rd party services
  - Review SP program
  - On-site inspection
  - Contracts and enforce implementation
  - SLA assurance
  - Audit report internal/external
  - Review from customer/employees and interviews
  - NDA
  - BCP
  - SAS70/SOC reports

Risk Management Frameworks

- NIST SP 800 Series has CSF 800-53 and RMF 800-37
- ISO/IEC 27005 ISRMS (Specific to Information Security unlike ISO31000)
- COSO involves risk management for financial industry targeting SOX compliance to prevent fraud
- COBIT involves risk management for IT governance
- OCTAVE
- SABSA

-ITIL is non-risk oriented

-SPAM Unwanted advertisement emails, may include malware and Trojan horse
-Typo squatting familiar same url
-Phish is target email to organization to deceive
-Smishing is SMS based mislead info
-Vishing is fake phone calls
-Spear phishing direct to particular person or org

-Skimming is the fake device (numberpad e,g) inserted to get information
-Whaling spearing to top executives
-Tailgate is sneak behind someone
-Influence campaign is mass public opinion change over fake news
-HOAX fake msg asking to act and install or do an IT task

Prevention of Security Threats

- Establish and Maintain security of technical and physical controls
- Awareness, Education, and Training Program
  - Gamification
  - Effective evaluation of awareness programs