Risk Mitigation

- Risk mitigation includes all possible solutions for reducing the **probability of risk** and limiting the impact of a risk if it occurs
- It should identify the mitigation strategies for the risks that fall outside the department's **risk tolerance** and provide an understanding of the level of risk with controls and treatments
- It identifies the priority order in which individual risks should be **mitigated**, **monitored**, and **reviewed**

Risk Mitigation Strategies

1. Risk Assumption
2. Risk Avoidance
3. Risk Limitation
4. Risk Planning
5. Research and Acknowledgment
6. Risk Transference

Control the Risks

- Identify all existing security controls that can help organizations in **reducing security risks**
- Recommend any new security controls the organization must implement
- Use the results of vulnerability and threat assessment to minimize risks, as risks are directly proportionate to them

Some of the security controls that help in reducing risks include:

1. Impart **security awareness** to employees
2. Place up-to-date hardware and software **security solutions** such as IDS, firewall, honeypot, and DMZ
3. Strengthen network, account, application, device, and **physical security** across the organization
4. Implement **strict access controls** and security policies
5. Deploy **encryption** for all data transfers
6. Implement an **appropriate incident handling** and response plan

Notes:

Risk Calculation Formulas

- Many types of calculations exist
- Not every risk can be invested in equally
- Risk treatments should be commensurate with the value of the assets at risk
- Risk formulas allow security professionals to dimension risk

- **Asset Value (AV)**: The value you have determined an asset to be worth
- **Exposure Factor (EF)**: The estimated percentage of damage or impact that a realized threat would have on the asset
- **Single Loss Expectancy (SLE)**: The projected loss of a single event on an asset
- **Annual Rate if Occurrence (ARO)**: The estimated number of times over a period the threat is likely to occur
- **Annualized Loss Expectancy (ALE)**: The projected loss to the asset based on an annual estimate

Quantitative Risk vs. Qualitative Risk

Qualitative

A subjective assessment

- Qualitative risk analysis focuses on mapping the perceived impact of a specific event occurring to a risk rating agreed upon by the organization
- Most methodologies use interrelated elements such as threats, vulnerabilities, and controls

Quantitative

A numeric assessment

- Quantitative risk analysis focuses on mapping the probability of a specific event occurring to the perceived cost of the event

This approach employs two fundamental elements:

- the probability of an event occurring
- the likely loss should it occur

Annual rate of occurrence X Single loss expectancy = Annualized loss expectancy

Notes: