



Risk Controls and Mitigations

THREAT MANAGEMENT

Risk Controls

 Cybersecurity professionals work to minimize risk to the organization through risk management and controls

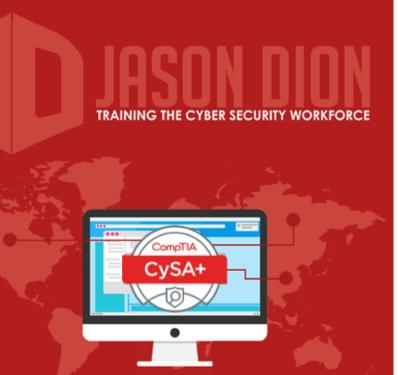
- Four ways to handle risk:
 - Risk Acceptance
 - Risk Avoidance
 - Risk Mitigation
 - Risk Transference



RISK ACCEPTANCE

 Organization accepts the risk associated with a system's vulnerabilities and their associated risks

 Risk acceptance is common when the risk is low enough to not apply countermeasures, or adequate countermeasures have already been applied



RISK AVOIDANCE

 Risk is too high to accept, so the system configuration or design is changed to avoid the risk associated with a specific vulnerability

Example:

 Utilizing Windows XP is too dangerous, so we install Windows 10 instead to avoid the risk of an unsupported operating system



RISK MITIGATION

 Main goal of security is to minimize risk to a level acceptable to the organization

 Our goal is not necessarily to <u>eliminate</u> all risks...

 By adding risk controls, we can mitigate the risk down to an acceptable level

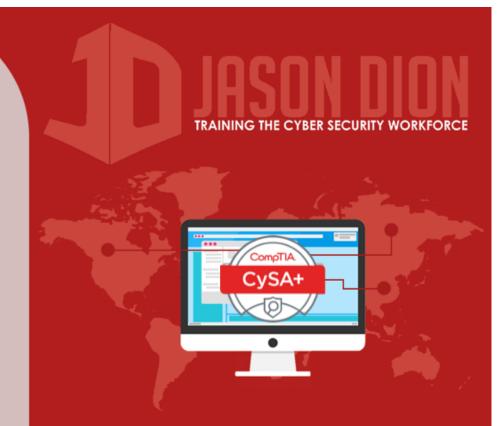


RISK TRANSFERENCE

 If the organization cannot afford to accept, avoid, or mitigate the risk, they can transfer the risk to another business

Example:

• If the organization is concerned that it would be too costly to recover from a flood, they can purchase flood insurance



RISK CONTROLS

- Technical controls
 - Systems, devices, software, and settings used to enforce CIA requirements
 - Examples
 - Using firewalls, IDS, and IPS
 - Installing antivirus and endpoint security
- Operational controls
 - Practices and procedures to increase security
 - Examples
 - Conducting penetration tests
 - Utilizing standard operating procedures

