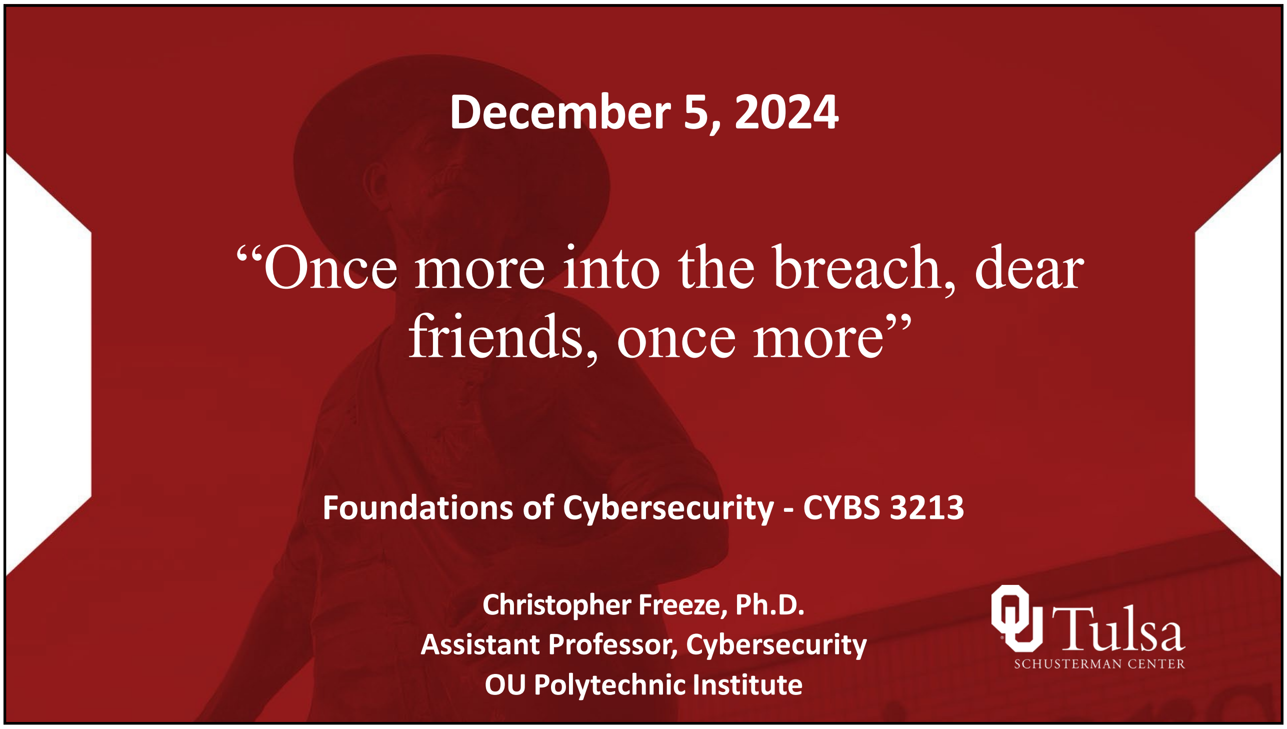


December 5, 2024

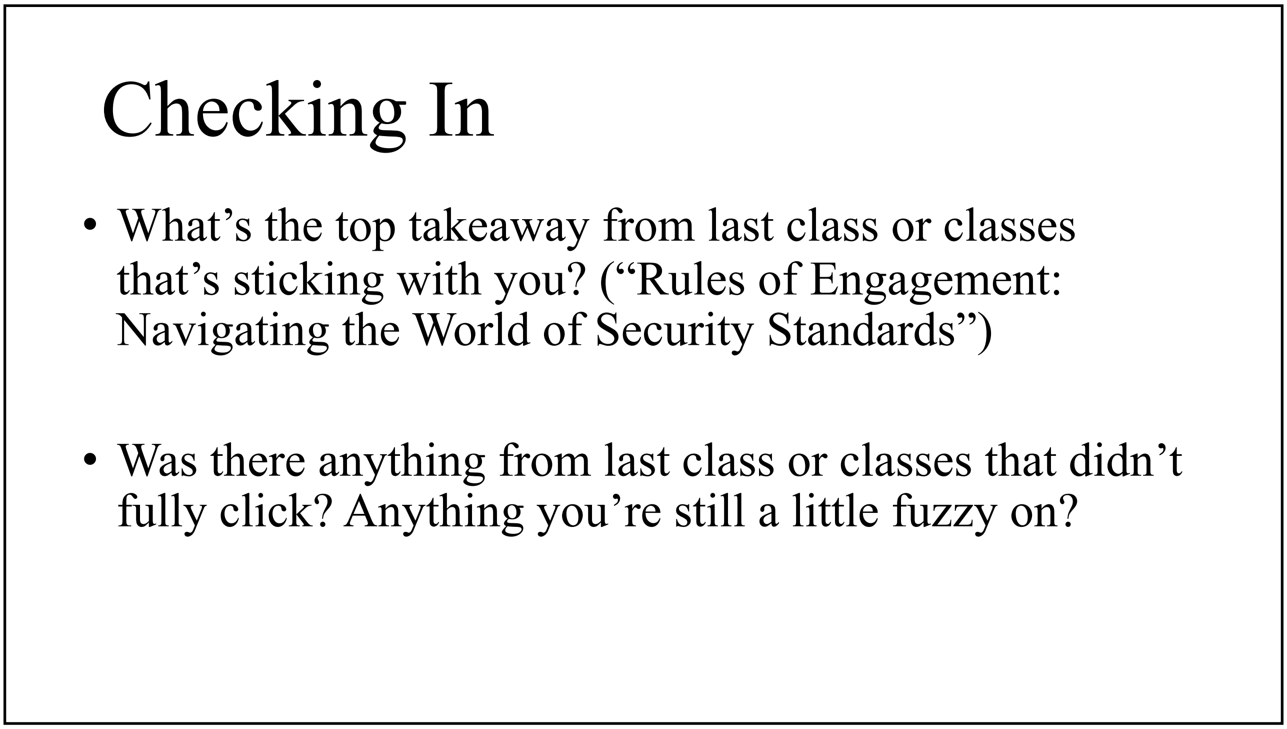
“Once more into the breach, dear friends, once more”

Foundations of Cybersecurity - CYBS 3213

Christopher Freeze, Ph.D.
Assistant Professor, Cybersecurity
OU Polytechnic Institute

Tulsa
SCHUSTERMAN CENTER

1



Checking In

- What’s the top takeaway from last class or classes that’s sticking with you? (“Rules of Engagement: Navigating the World of Security Standards”)
- Was there anything from last class or classes that didn’t fully click? Anything you’re still a little fuzzy on?

2

Learning Outcomes

1. Describe common causes of data breaches and evaluate appropriate internal and external escalation paths.
2. Classify data using organizational security levels (e.g., public, private, confidential).
3. Learn to identify, analyze, and manage risks by calculating risk severity, conducting both qualitative and quantitative risk assessments, and developing strategies to mitigate, accept, transfer, or avoid risks in alignment with organizational goals.

3

Data Breaches & Privacy

A data breach occurs when private or confidential information is exposed through unauthorized access. This applies to data stored internally or with external vendors. Common causes include:

1. Malicious hacking attacks
2. Lost/stolen devices (laptops, phones, USB drives)
3. Employee mistakes (like leaving passwords exposed)
4. Security system or policy failures

4

Data Breaches & Privacy

Breach Notifications Mandatory breach notifications inform affected individuals so they can protect themselves (like changing passwords or canceling cards). Key steps include:

1. Understanding legal requirements (all 50 states have specific rules)
2. Contacting law enforcement
3. Informing relevant stakeholders
4. Critical point: Affected individuals should be notified before the media learns of the breach.

5

Data Classifications and Privacy Technologies

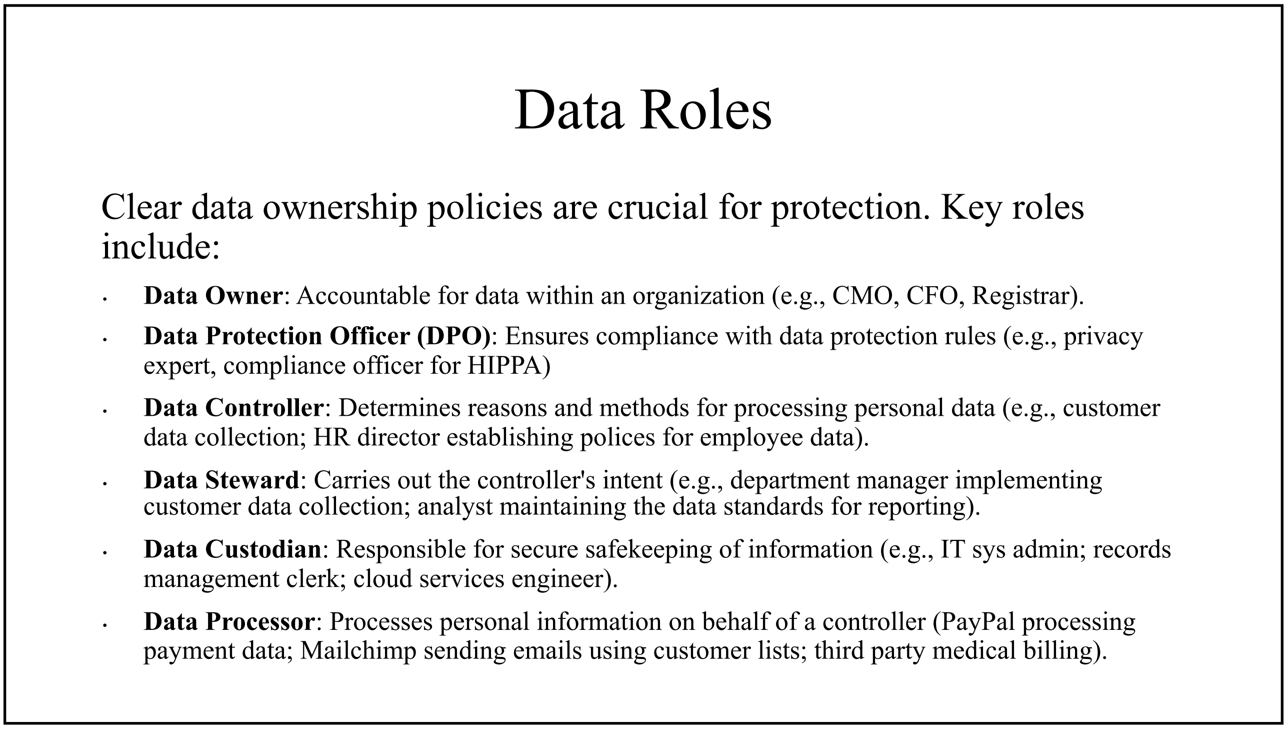
Data Classifications - Data classification helps organizations manage information security. From least to most restrictive:

- Public: Information freely available to everyone.
- Proprietary: Belongs to the company but not highly sensitive.
- Private: Personal information with limited access.
- Confidential: Sensitive data requiring strict protection.
- Sensitive: Highly restricted information with the tightest controls.

At what stages does data need to be protected?

- At rest; In transit; In Use

6

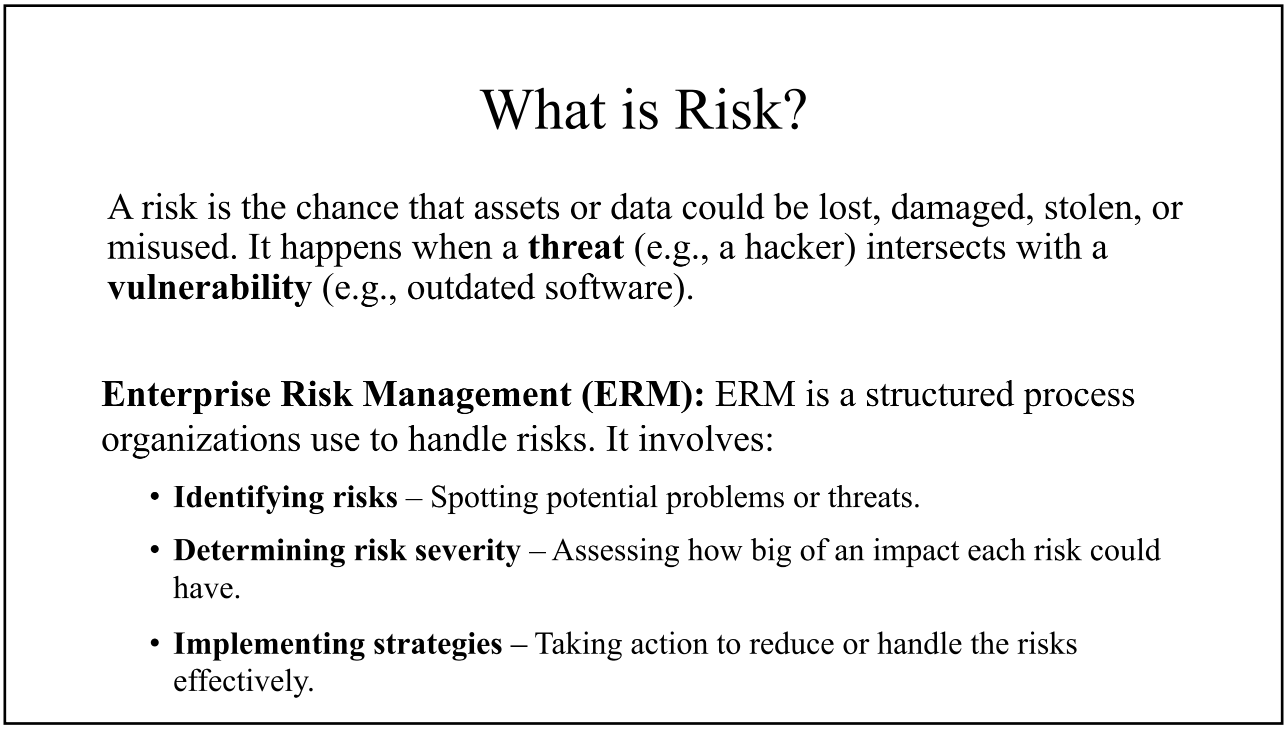


Data Roles

Clear data ownership policies are crucial for protection. Key roles include:

- **Data Owner**: Accountable for data within an organization (e.g., CMO, CFO, Registrar).
- **Data Protection Officer (DPO)**: Ensures compliance with data protection rules (e.g., privacy expert, compliance officer for HIPPA)
- **Data Controller**: Determines reasons and methods for processing personal data (e.g., customer data collection; HR director establishing polices for employee data).
- **Data Steward**: Carries out the controller's intent (e.g., department manager implementing customer data collection; analyst maintaining the data standards for reporting).
- **Data Custodian**: Responsible for secure safekeeping of information (e.g., IT sys admin; records management clerk; cloud services engineer).
- **Data Processor**: Processes personal information on behalf of a controller (PayPal processing payment data; Mailchimp sending emails using customer lists; third party medical billing).

7



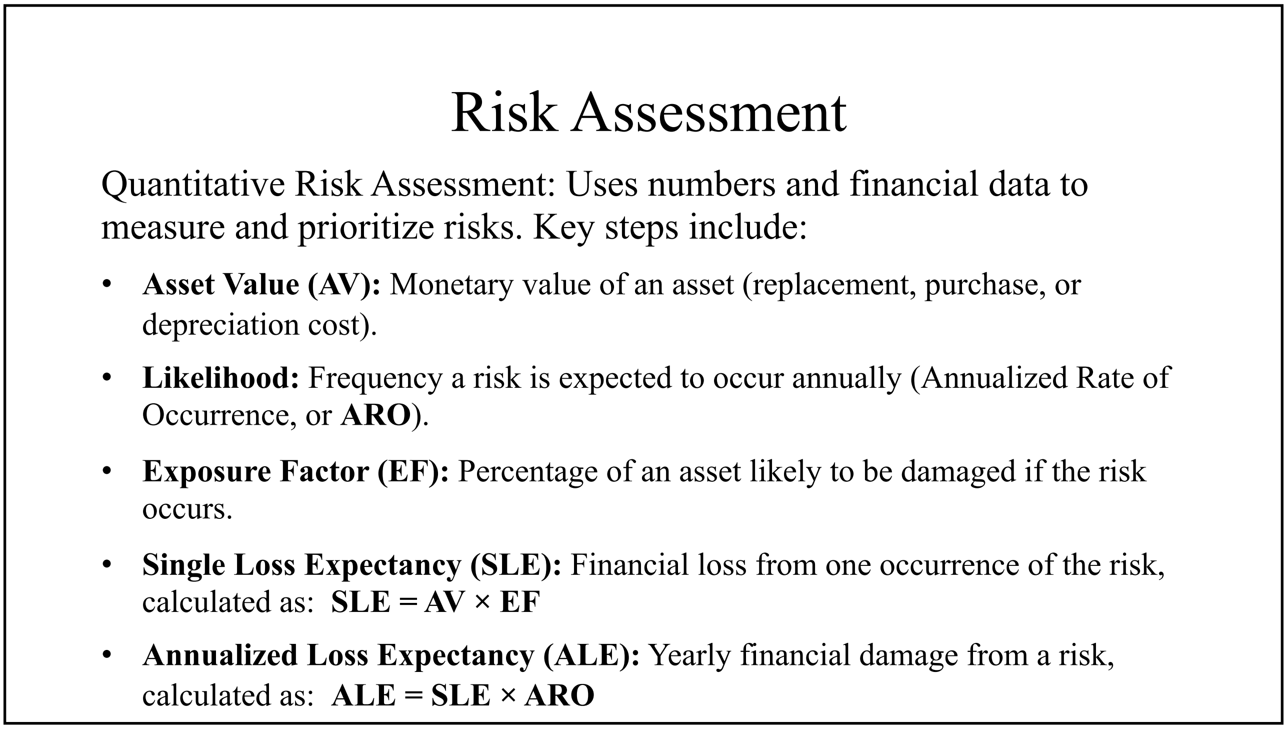
What is Risk?

A risk is the chance that assets or data could be lost, damaged, stolen, or misused. It happens when a **threat** (e.g., a hacker) intersects with a **vulnerability** (e.g., outdated software).

Enterprise Risk Management (ERM): ERM is a structured process organizations use to handle risks. It involves:

- **Identifying risks** – Spotting potential problems or threats.
- **Determining risk severity** – Assessing how big of an impact each risk could have.
- **Implementing strategies** – Taking action to reduce or handle the risks effectively.

8

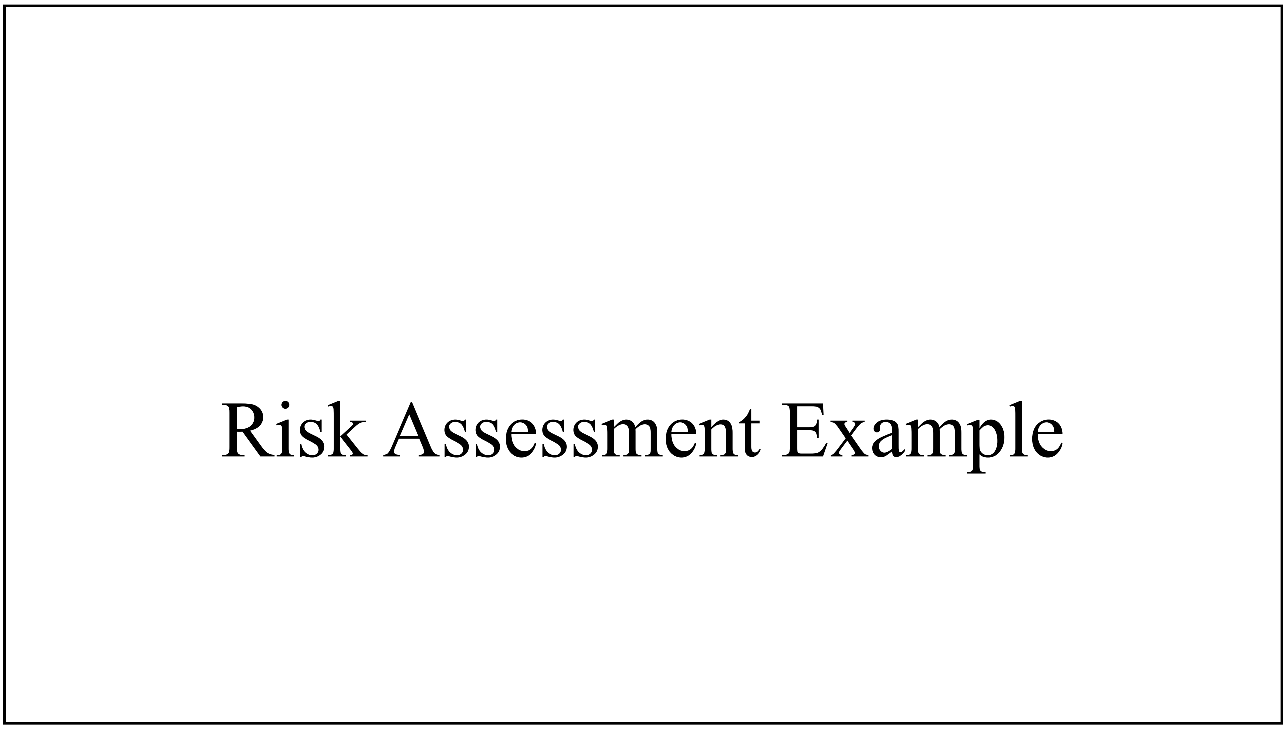


Risk Assessment

Quantitative Risk Assessment: Uses numbers and financial data to measure and prioritize risks. Key steps include:

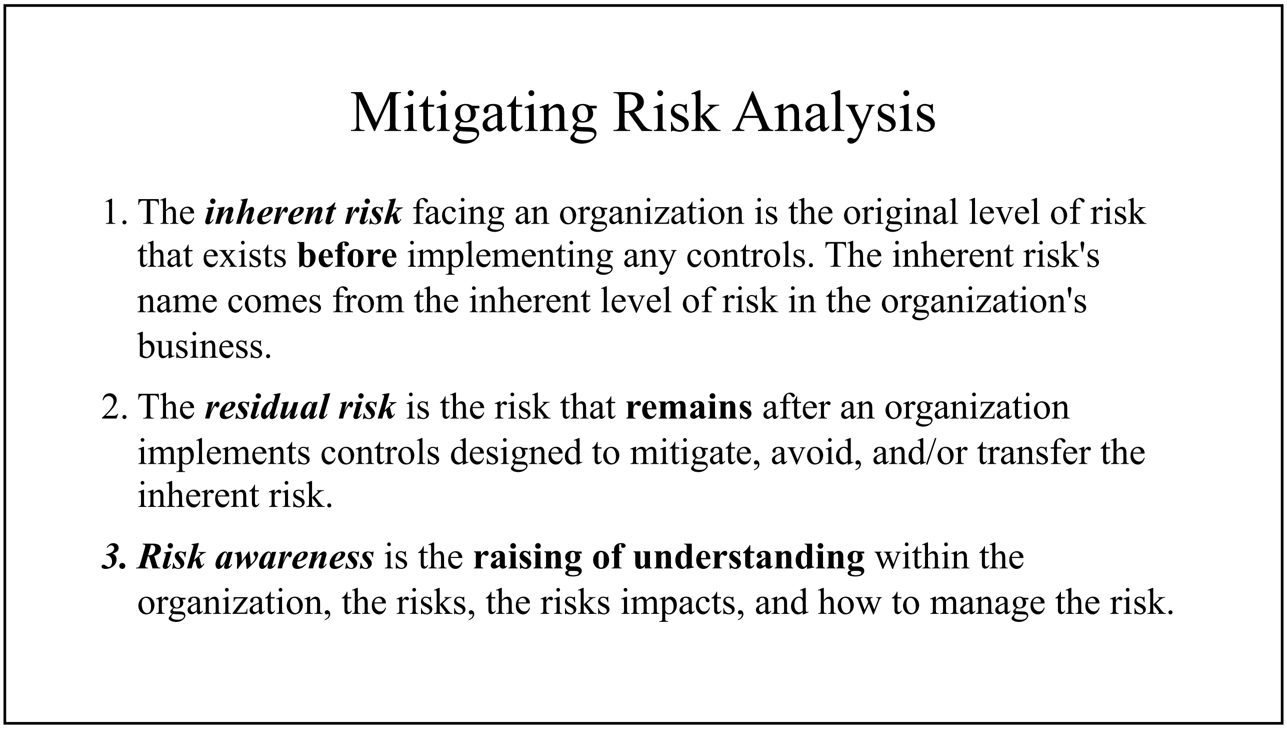
- **Asset Value (AV):** Monetary value of an asset (replacement, purchase, or depreciation cost).
- **Likelihood:** Frequency a risk is expected to occur annually (Annualized Rate of Occurrence, or **ARO**).
- **Exposure Factor (EF):** Percentage of an asset likely to be damaged if the risk occurs.
- **Single Loss Expectancy (SLE):** Financial loss from one occurrence of the risk, calculated as: **SLE = AV × EF**
- **Annualized Loss Expectancy (ALE):** Yearly financial damage from a risk, calculated as: **ALE = SLE × ARO**

9



Risk Assessment Example

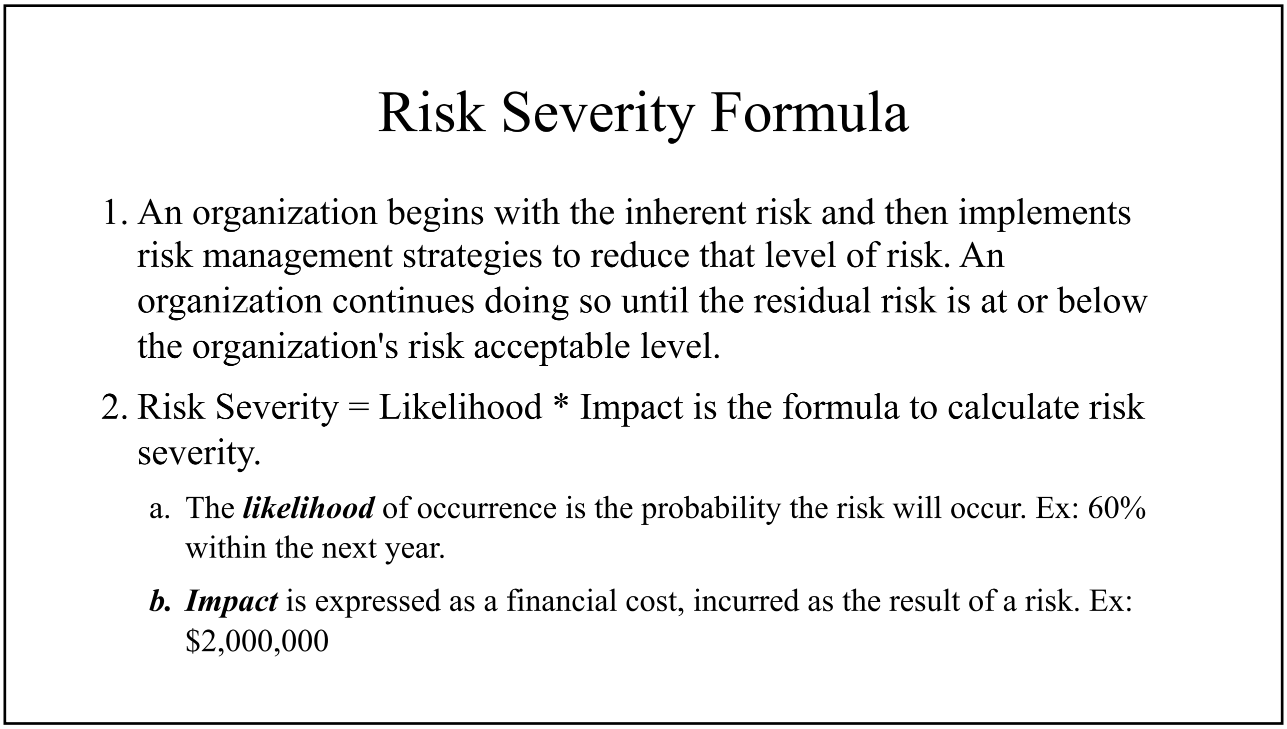
10



Mitigating Risk Analysis

1. The ***inherent risk*** facing an organization is the original level of risk that exists **before** implementing any controls. The inherent risk's name comes from the inherent level of risk in the organization's business.
2. The ***residual risk*** is the risk that **remains** after an organization implements controls designed to mitigate, avoid, and/or transfer the inherent risk.
3. ***Risk awareness*** is the **raising of understanding** within the organization, the risks, the risks impacts, and how to manage the risk.

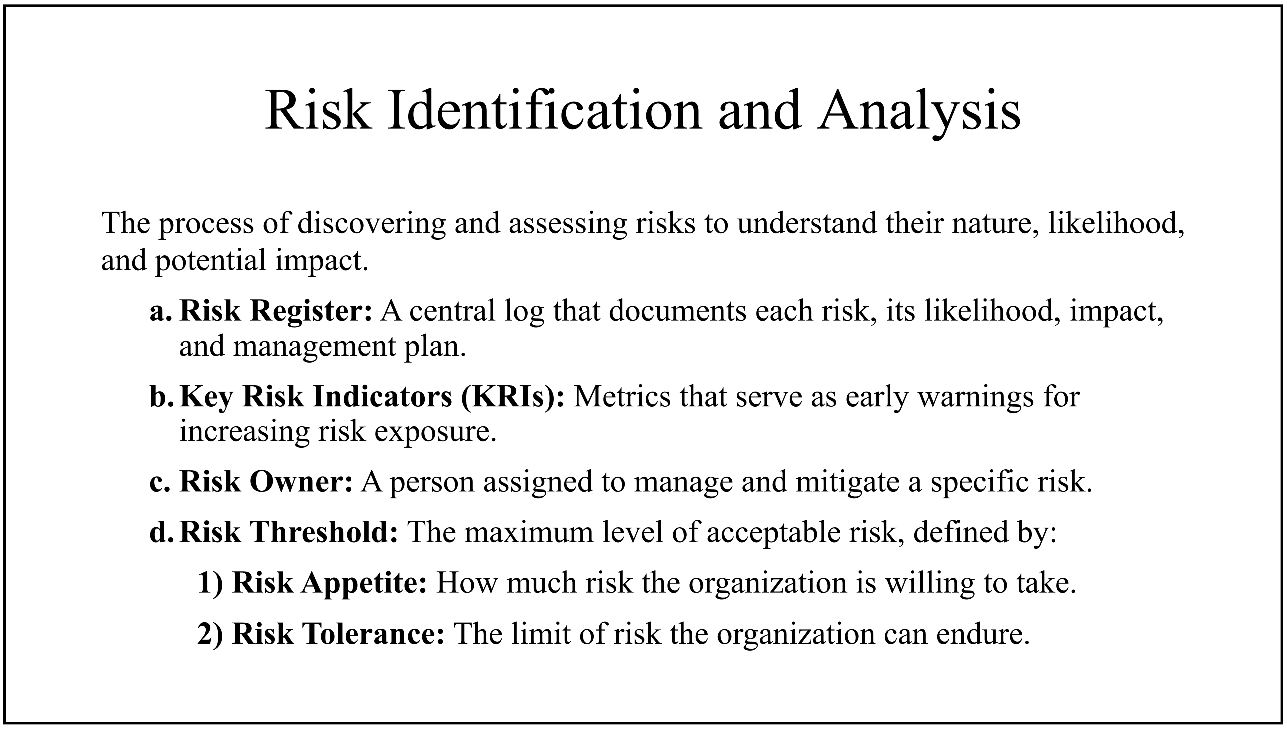
11



Risk Severity Formula

1. An organization begins with the inherent risk and then implements risk management strategies to reduce that level of risk. An organization continues doing so until the residual risk is at or below the organization's risk acceptable level.
2. Risk Severity = Likelihood * Impact is the formula to calculate risk severity.
   a. The ***likelihood*** of occurrence is the probability the risk will occur. Ex: 60% within the next year.
   b. ***Impact*** is expressed as a financial cost, incurred as the result of a risk. Ex: $2,000,000

12



Risk Identification and Analysis

The process of discovering and assessing risks to understand their nature, likelihood, and potential impact.

a. **Risk Register:** A central log that documents each risk, its likelihood, impact, and management plan.

b. **Key Risk Indicators (KRIs):** Metrics that serve as early warnings for increasing risk exposure.

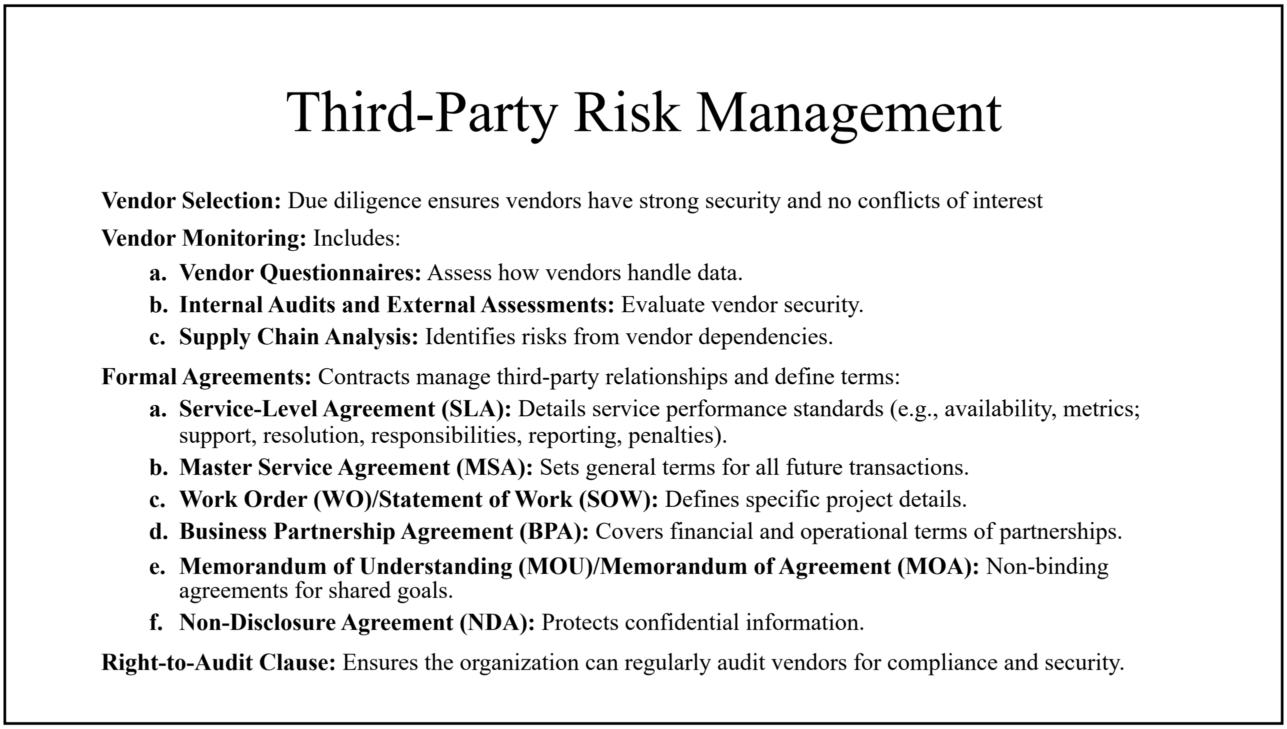
c. **Risk Owner:** A person assigned to manage and mitigate a specific risk.

d. **Risk Threshold:** The maximum level of acceptable risk, defined by:

  1) **Risk Appetite:** How much risk the organization is willing to take.

  2) **Risk Tolerance:** The limit of risk the organization can endure.

13



Third-Party Risk Management

Vendor Selection: Due diligence ensures vendors have strong security and no conflicts of interest

Vendor Monitoring: Includes:

a. **Vendor Questionnaires:** Assess how vendors handle data.
b. **Internal Audits and External Assessments:** Evaluate vendor security.
c. **Supply Chain Analysis:** Identifies risks from vendor dependencies.

Formal Agreements: Contracts manage third-party relationships and define terms:

a. **Service-Level Agreement (SLA):** Details service performance standards (e.g., availability, metrics; support, resolution, responsibilities, reporting, penalties).
b. **Master Service Agreement (MSA):** Sets general terms for all future transactions.
c. **Work Order (WO)/Statement of Work (SOW):** Defines specific project details.
d. **Business Partnership Agreement (BPA):** Covers financial and operational terms of partnerships.
e. **Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA):** Non-binding agreements for shared goals.
f. **Non-Disclosure Agreement (NDA):** Protects confidential information.

Right-to-Audit Clause: Ensures the organization can regularly audit vendors for compliance and security.

14

Gap Analysis and Business Impact Analysis

Gap Analysis: A process to compare current performance or controls with desired standards. In security, it identifies weaknesses, helps prioritize fixes, and ensures compliance with standards or regulations

Key BIA Metrics:

- **Mean Time to Repair (MTTR):** Average time needed to fix a resource after failure.
- **Mean Time Between Failures (MTBF):** Average time between resource failures during normal operation.
- **Recovery Time Objective (RTO):** Target time to restore operations after a disruption.
- **Recovery Point Objective (RPO):** Maximum acceptable data loss measured in time (e.g., last backup point).

15

As part of his role, Augie is responsible for implementation of business rules related to data, as well as for storage, and use of data and datasets. What data-related role does Augie hold?

a. Data owner

✅ b. Data custodian

c. Data processor

d. Data subject

16

Brian recently conducted a risk mitigation exercise and has determined the level of risk that remains after implementing a series of controls. What term best describes this risk?

a. Inherent risk

b. Control risk

c. Risk appetite

✅ d. Residual risk

17

Gary is beginning his risk assessment for the organization and has not yet begun to implement controls. What risk does his organization face?

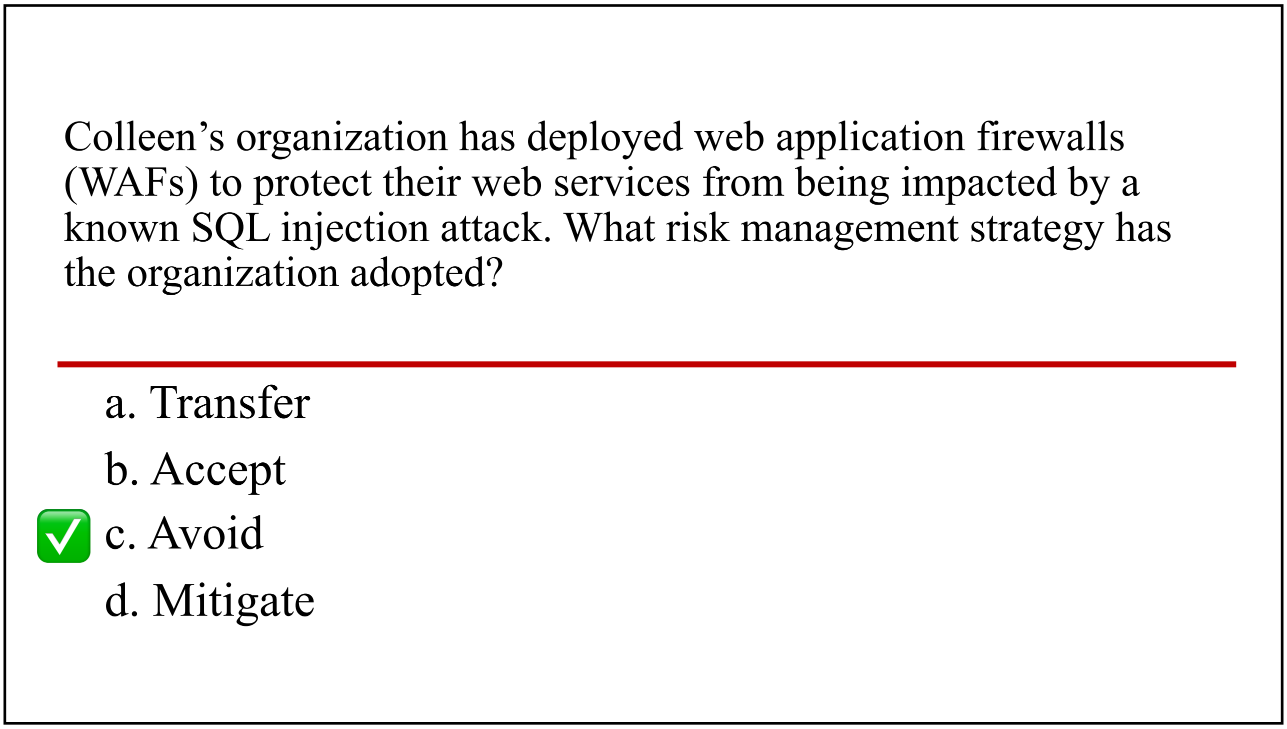
a. Residual risk

b. IP theft risk

c. Multiparty risk

✅ d. Inherent risk

18



Colleen’s organization has deployed web application firewalls (WAFs) to protect their web services from being impacted by a known SQL injection attack. What risk management strategy has the organization adopted?

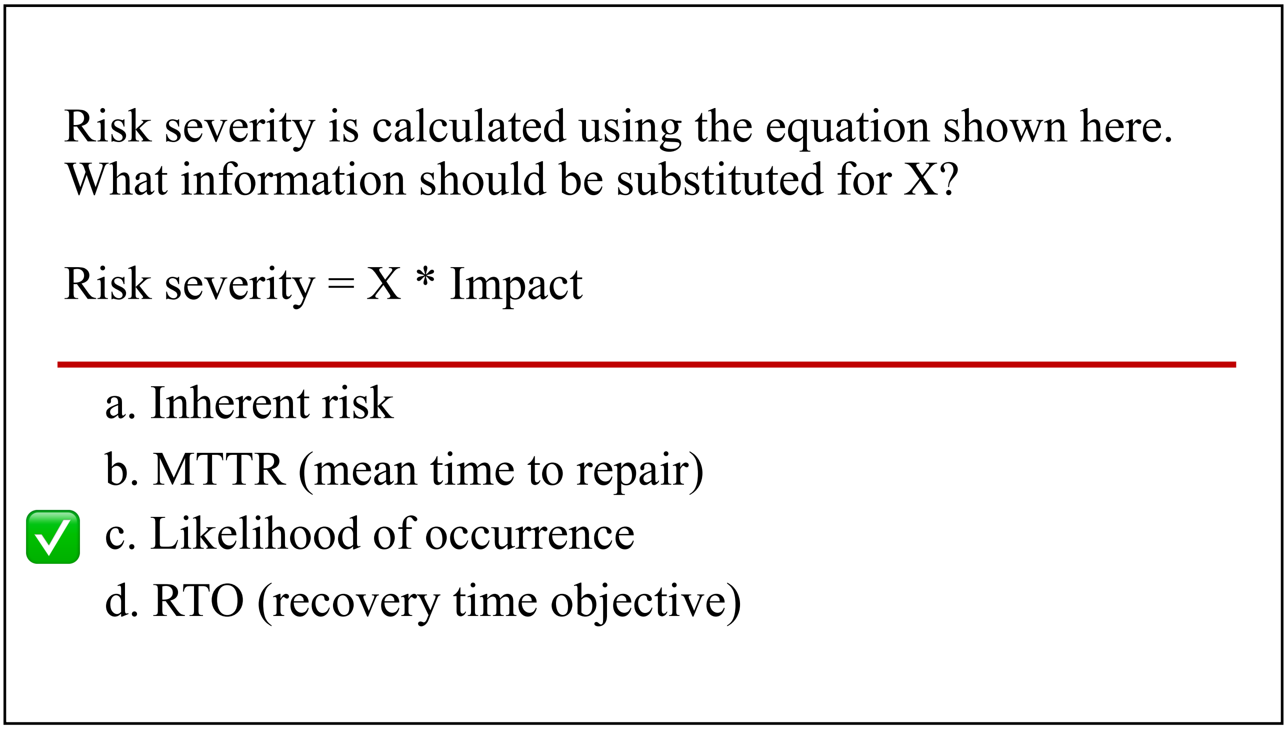
a. Transfer

b. Accept

✅ c. Avoid

d. Mitigate

19



Risk severity is calculated using the equation shown here. What information should be substituted for X?

Risk severity = X * Impact

a. Inherent risk

b. MTTR (mean time to repair)

✅ c. Likelihood of occurrence

d. RTO (recovery time objective)

20

Henry's organization has set their RTO to 12 hours. What does this mean?

a. Outages must be less than 6 hours long.

✅ b. Recovery from outages should take less than 12 hours.

c. Outages longer than 12 hours will require fail over to a warm site.

d. SLAs for third-party services should specify a 12 hour MTBF.

21

Irene's organization needs to follow PCI DSS standards. If she engages a third party to assess this, what type of audit is she having performed?

a. An internal regulatory audit

b. An external regulatory audit

c. An internal compliance audit

✅ d. An external compliance audit

22

Olivia’s cloud service provider claims to provide zero data loss from storage, and Olivia’s company wants to take advantage of that service because loss of data would be extremely costly for the business. What business agreement can Oliva put in place to help ensure that the reliability that the vendor advertises is maintained?

a. An MOU (Memorandum of Understanding)

✅ b. An SLA (Service Level Agreement)

c. An MSA (Master service Agreement)

d. A BPA (Business Partnership Agreement)

23

What process reviews control objectives for an organization, system, or service to determine if controls do not meet the control objectives?

a. A penetration test

✅ b. A gap analysis

c. A Boolean analysis

d. A risk analysis

24

Which of the following is not a commonly used business data classification?

a. Sensitive

b. Confidential

✅ c. Top Secret

d. Public

25

Which of the following techniques attempts to predict the likelihood a threat will occur and assigns monetary values should a loss occur?

a. Change management

b. Vulnerability assessment

c. Qualitative risk assessment

✅ d. Quantitative risk assessment

26

You have an asset that is valued at $16,000, the exposure factor of a risk affecting that asset is 35 percent, and the annualized rate of occurrence is 75 percent. What is the SLE?

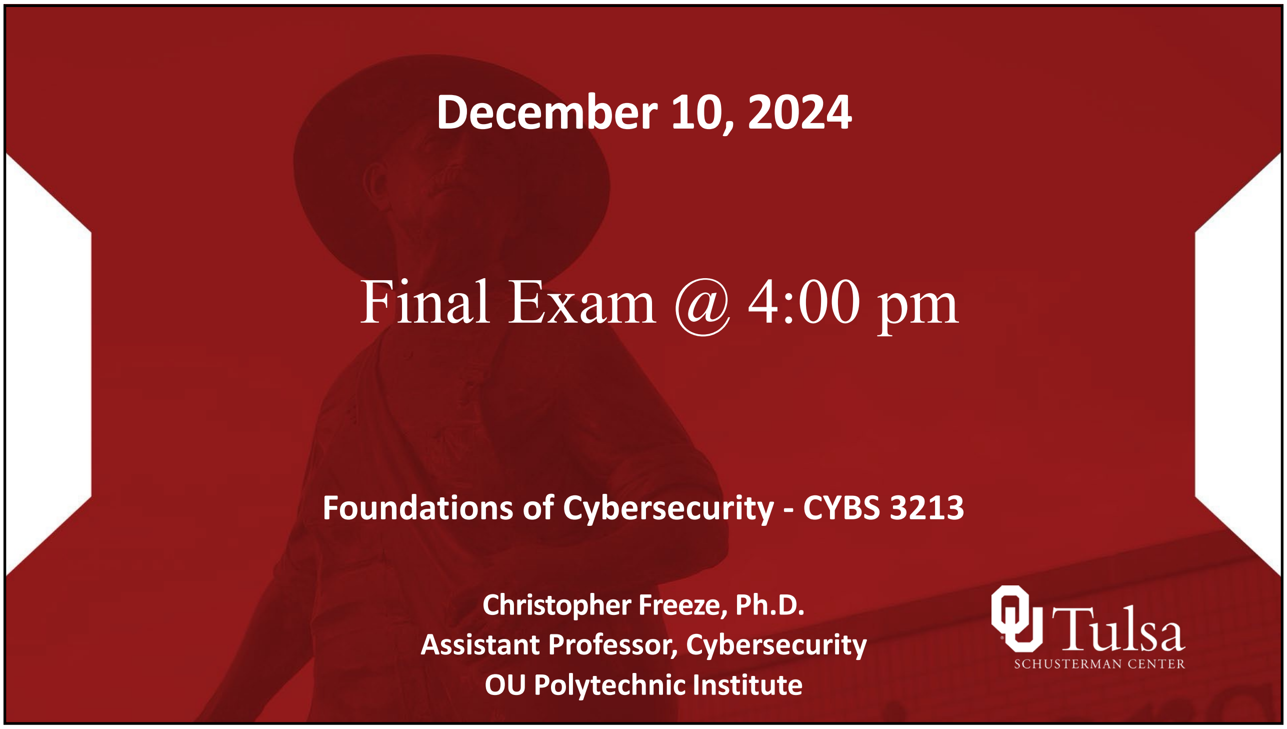
✅ a. $5,600

b. $5,000

c. $4,200

d. $3,000

27



December 10, 2024

Final Exam @ 4:00 pm

Foundations of Cybersecurity - CYBS 3213

Christopher Freeze, Ph.D.
Assistant Professor, Cybersecurity
OU Polytechnic Institute

28