# Risk Assessment


## CSI-604 - Information Security

# Course Outline

**Course Name: Information Security**
**Credit Hours:** 3(3-0)
**Prerequisites: Data Communication and Computer Networks**
**Course Outline:**
Basic notions of confidentiality, integrity, availability; authentication models; protection models; security kernels; Encryption, Hashing and Digital Signatures; audit; intrusion detection and response; database security, hostbased and network-based security issues operational security issues; physical security issues; personnel security; policy formation and enforcement; access controls; information flow; legal and social issues; identification and authentication in local and distributed systems; classification and trust modeling; risk assessment
**Reference Materials:**
1. *Computer Security: Art and Science*, Matthew Bishop
2. *Cryptography and Network Security* by William Stalling 6th Edition, 2012
3. *Principles of Information Security* 3rd E by Michael E. Whitman and Herbert J. Mattord

# Risk Assessment

- Risk assessment is a fundamental process in information security that helps organizations identify, analyze, and mitigate potential risks to their digital assets, systems, and data.
- It's a structured approach to understanding and managing security threats and vulnerabilities.
- Here's an overview of the key steps and concepts in risk assessment in information security:

# Risk Assessment cont…

- **Identify Assets:** Begin by identifying all the assets within your organization.
- These include hardware (e.g., servers, computers, mobile devices), software, data, networks, and even human resources.

# Risk Assessment cont…

- **Identify Threats and Vulnerabilities:** Threats are potential events or incidents that could harm your assets or data (e.g., malware, data breaches).
- Vulnerabilities are weaknesses or gaps in your security that can be exploited by threats (e.g., unpatched software, weak passwords).

# Risk Assessment cont…

- **Assess the Impact:** Determine the potential impact or harm that each threat could have on your assets.
- This includes assessing the loss of data, downtime, financial losses, reputational damage, and regulatory penalties.

# Risk Assessment cont…

- **Assess Likelihood:** Evaluate the likelihood or probability of each threat exploiting a vulnerability.
- This often involves considering historical data, industry trends, and expert judgment.

# Risk Assessment cont...

- **Calculate Risk:** Risk is calculated as the product of impact and likelihood.
- The formula is: Risk = Impact x Likelihood.
- This quantifies the level of risk associated with each threat-vulnerability pair.

# Risk Assessment cont…

- **Prioritize Risks:** Rank the identified risks based on their level of criticality.
- High-risk issues that have a significant impact and a high likelihood should be addressed urgently.

# Risk Assessment cont…

- **Mitigation Strategies:** Develop strategies to mitigate or reduce the identified risks.
- This may involve implementing security controls, policies, or procedures to reduce vulnerabilities or minimize the impact of threats.

# Risk Assessment cont...

- **Residual Risk:** After implementing mitigation measures, reassess the risk.
- The remaining risk is known as “residual risk”.
- It's important to ensure that residual risk is at an acceptable level.

# Risk Assessment cont…

- **Documentation:** Document the entire risk assessment process, including the identified risks, their assessment, mitigation strategies, and ongoing monitoring and review plans.

# Risk Assessment cont...

- **Ongoing Monitoring and Review:** Information security risks are dynamic and can change over time.
- Regularly monitor and review the risk assessment to account for new threats, vulnerabilities, or changes in the organization's environment.

# Risk Assessment cont…

- **Compliance and Reporting:** Depending on your industry and regulatory requirements, you may need to report on your risk assessment process and outcomes.
- Compliance often involves demonstrating that you have identified and managed risks appropriately.

# Risk Assessment cont…

- **Risk Management Frameworks:** Many organizations follow established risk management frameworks, such as ISO 27001, NIST Cybersecurity Framework, or FAIR (Factor Analysis of Information Risk), to guide their risk assessment and management processes.

# Risk Assessment cont…

- Effective risk assessment is a critical component of a comprehensive information security program.
- It helps organizations make informed decisions about where to allocate resources for security improvements and ensures that security measures are aligned with business objectives and risk tolerance.