# Milestone 2: Risk & Operational Assessments

## Objective:

### Risk Assessments

1. Identify potential risks: Risk assessment helps to identify potential risks that could impact the organization's assets, such as data, systems, employees, and reputation.
2. Prioritize risks: Risk assessment helps to prioritize risks based on their likelihood and impact so that the organization can allocate resources more effectively to mitigate the highest-priority risks.
3. Reduce vulnerabilities: Risk assessment helps to identify vulnerabilities in the organization's systems and processes so that they can be addressed proactively to reduce the risk of a security breach.
4. Compliance: Risk management helps organizations to comply with regulatory requirements, such as HIPAA, PCI DSS, and GDPR, which require risk assessments and risk management programs to protect sensitive information.
5. Cost-effective: Risk management helps organizations to reduce the cost of security incidents by proactively mitigating risks before they occur. This can save the organization money on legal fees, data recovery costs, and reputational damage.
6. Continuous improvement: Risk assessment and risk management are ongoing processes that help organizations to continuously improve their security posture by identifying new risks and addressing them proactively.

### Operational Assessments

1. Process Analysis: Evaluate the organization's core processes to identify bottlenecks, inefficiencies, and opportunities for improvement.
2. Performance Metrics: Measure and analyze key performance indicators (KPIs) to assess how well the organization is meeting its goals.

## Instructions:

### Step 1: Risk Assessment

As a team, you will create a comprehensive risk management plan for the network you designed in the previous step. The document should be professional in its formatting and be easy to understand and navigate.

Your plan should at a minimum contain the following:

1. Identify assets: Identify the assets that need to be protected, such as servers, databases, applications, and network devices.
2. Identify threats: Identify potential threats that could impact the assets, such as malware, phishing attacks, insider threats, and denial-of-service attacks.
3. Assess vulnerabilities: Assess the vulnerabilities of the assets by conducting vulnerability scans, penetration testing, and other security assessments.
4. Determine likelihood and impact: Determine the likelihood and impact of each potential risk based on the identified threats and vulnerabilities. This can be done using a risk matrix or other risk assessment tools.
5. Prioritize risks: Prioritize the risks based on their likelihood and impact and assign a risk level to each risk.
6. Develop mitigation strategies: Develop mitigation strategies to reduce the risk level of each identified risk. Mitigation strategies can include implementing security controls such as firewalls, intrusion detection and prevention systems, access controls, and encryption.
7. Implement controls: Implement the selected security controls to reduce the risk level of each identified risk.
8. Monitor and review: Monitor the network and services regularly to detect any new vulnerabilities and to ensure that the implemented security controls are effective.

In addition to a written document, you should create a spreadsheet to document any risks you have identified and any information pertaining to that risk.

## Step 2: Operational Assessments

1. Complete one of the operational assessments from Chapter 56: Operational Assessments

## Submission Requirements

☐ 60 Points - Submit your comprehensive risk management documents to Learning Suite. Submit documents in the appropriate file format and file security measures.

☐ 40 Points - Submit your completed Operational Assessment. Submit documents in the appropriate file format and file security measures.