

CYB 420 4-1 Project Two Milestone One: Project Charter

Andree Salvo

Southern New Hampshire University

CYB 420

Instructor: William Mitchell

Project Name: Project Charter
Project Charter

Project Description
Create a mission statement to explain the project goal of addressing one vulnerability for each of the three risk domains (people, process, and technology).
My project aims to make ACME more secure by addressing a major weakness across three areas: people, process, and technology. I will do this through specific training, better policies, and stronger network controls. This will help create a safer environment, reduce mistakes, ensure consistent actions, and prevent threats from spreading in ACME's network before they can.

Organization

Prompt	Answer
Discuss the business needs you will meet by completing this project.	Given business needs, ACME relies on HR, Finance, Records, and several core systems. The company needs stronger protection against social engineering, unauthorized access, and unclear security procedures. Improving training, policies, and the network layout will help keep ACME data safe, prevent mistakes, and support business operations as the company continues to grow further.

Prompt	Answer
Explain your project's methods of scalability .	For scalability, Training can be reused for new hires, and policies can be updated as new systems or hardware are added. Standardized network configurations make it easier to add new switches or servers, and centralized management lets ACME update multiple devices from a single location. Security monitoring tools can automatically scale to cover new equipment, and the patching process can include new devices without requiring further changes. This keeps ACME's security flexible and ready for future growth.

Project Completion

Prompt	Answer
Explain the scope of what will be delivered at the end of the project.	<p>The scope that I will deliver at the end of my project is:</p> <ul style="list-style-type: none"> - A security awareness training program that teaches employees how to recognize phishing attempts and social engineering tactics, especially for those targeting HR, Finance, and Records workstations. - Full set of standardized security policies, including physical security requirements for locked doors, IT equipment closets, and the second-floor server area, along with rules for data handling and access management. - Improved network segmentation with VLANs and ACLs to separate HR, Finance, Records, and IT traffic, along with regular update practices for servers and workstations to reduce vulnerabilities. - Clear documentation so the company can maintain these changes going forward.

Prompt	Answer
Assess the potential business impacts of the project.	These upgrades will reduce social engineering, improve staff compliance with procedures, and block attackers from moving freely across the network. This will help protect sensitive systems, reduce downtime, and strengthen ACME's security posture.