# IT 552 Final Project Case Document

## **Scenario**

You have just been hired as the new chief information security officer for Multiple United Security Assurance (MUSA) Corporation, whose security posture is low. The first thing your chief executive officer tells you is that the information security team recently presented information emphasizing the importance of a strong security awareness program. As a result, you have been asked to develop a security awareness program for MUSA Corporation that consists of four major components:

1. Proposal Introduction
2. Security Policies Development
3. Continuous Monitoring Plan
4. Communication Plan

## Security Status

The information security team gave you the following details about MUSA Corporation’s security status:

* No annual cybersecurity awareness training, which is causing successful phishing and social engineering attacks
* No configuration change management policy (to reduce unintentional threats)
* No intrusion detection or prevention system
* No logs are being collected or analyzed
* No media access control policy
* No encryption or hashing to control data flow and unauthorized alteration of data
* A vulnerability assessment that is conducted every three years, which prevents accurate assessment of the security posture status
* High turnover and low morale among the employees (due to lack of employee readiness programs and work planning strategy)
* High number of theft reports and security incidents, which suggests there may be unethical or disgruntled employees
* No separation of duties or mandatory vacation policies (to mitigate intentional threats)

You will make recommendations for enhancing security policies, practices, and processes that are now contributing to a dysfunctional security culture. Your chief goal is to build a program that will foster a healthy security culture and ensure continuous improvement.