# IT 552 Case for Final Project

BACKGROUND:

You were just hired as the new chief information security officer for Multiple Unite Security Assurance (MUSA) Corporation whose security posture is low. The first thing your chief executive officer tells you is that they have recently seen a presentation by one of the information security team members emphasizing the importance of having a security awareness program. As a result, you have been asked to develop a security awareness program for MUSA Corporation based on the following 10 security gaps:

1. No annual cyber security awareness training, which is causing high phishing and social engineering attacks
2. No configuration change management policy (to reduce **unintentional threats**)
3. No intrusion detection/prevention system
4. Logs are not being collected or analyzed
5. No media access control policy
6. No encryption or hashing to control **data flow** and unauthorized alteration of data
7. Vulnerability assessment is conducted every three years; unable to assess the security posture status
8. High turnover and low morale among the employees (due to lack of **employee readiness** programs and work **planning strategy**)
9. High number of theft reports and security incidents; possible unethical/disgruntled employees
10. No segregation of duties or mandatory vacation policies (to mitigate **intentional threats**)

To that end, you will make recommendations for enhancing security policies, practices, and processes that are currently 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. Your task is to develop a security awareness program that consists of four major components:

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