# CS 305 Module Two Written Assignment Template

## Instructions

Replace the bracketed text with the relevant information in your own words. If you choose to include images or supporting materials, make certain to insert them in all the relevant locations in the document.

## Areas of Security

The VAPFD identifies the system within your network and any vulnerabilities found within; it will also prioritize any remedy for risks that could cause more significant problems in the system. Although this is based on the user/client input, all assets need to be identified, as well as all risks for each system.

## Areas of Security Justification

The inputs entered by the client can indeed create a vulnerable system; however, this can help by reducing the risks and, at the same time, increasing protection. This is why the importance of knowing the device on the network can help understand that the access could be by employees, Admin, or any user authorized by them.

For this to be accomplished, we need to understand the five risk factors: Appetite, tolerance, mitigation, residual risks, and business impact analysis.

## Code Review Summary

Before assessing any vulnerability, we need to gather as much information about the system as possible and ensure that any device has any services or open ports process that can't be manipulated. Another factor we should know to make sure no one from outside the company gains access to the system is understanding what type of software and drivers can be and should be approved for installation on any of the company devices.

## Mitigation Plan

A good mitigation plan must include all results from the Source Code Analysis. This analysis will provide the identification of the vulnerability from a few severe levels of threats. During the software lifecycle the use of mechanical tools Source Code Analysis can and should be used on different stages.

Only being able to identify vulnerabilities will not and cannot be enough for the developer to fix and roll out a project; they need to ensure that all possible bugs are dealt with as well fixed and that they go through the proper testing before any project is released. This will reduce the opportunity for attacks.