ISEC-635 Info Sec Operations Management Assignment 2 Guidelines

**Objectives**

Nowadays, security planning and operations management has become a top priority in small, medium and large organizations. This assignment aims to explore strategic preparedness through security operation contingency plans (i.e. business continuity, disaster recovery and incident response) for small and mid size organizations. The outcome for this assignment is to provide students the training on how to develop strategic contingency plans including business continuity, disaster recovery and incident response (CPM2). Moreover, this assignment will require students to construct and develop system specific plans for the protection of organizational intellectual property, the implementation of access controls, as well as patch and change management (CPM3). Students will explain the roles of personnel in planning and managing these specific plans including: board of directors, senior Management, Chief Information Security Officer (CISO), IT management (Chief Information Officer (CIO), IT Director, etc.), functional area managers, Information Security personnel, and end users (CPM4).

**Structure**

This security operations management assignment is designed to provide you with hands-on

experience solving real-world information security challenges. You will select an organization that you are familiar with to use as the basis for this assignment. It is recommended to base your assignment solution on the same company that you used for the first assignment in this course.

The project will consist of one executive summary and one recorded presentation. The presentation will require the preparation of a 15-minute presentation (using PowerPoint) on a specific company that addresses the issues noted below.

**Assignment 2 Guidelines**

Prepare a 15-minute presentation with an executive summary of your analysis and solution, focusing on the following guidelines:

1. Quick overview of a small to medium business that you are familiar with (current workplace, family business, etc.)
2. Description of the strategic contingency plans ***focusing on information security operations including: (a) business continuity, (b) disaster recovery and (c) incident response*** (CPM2). Ensure to separate the plans based on the following three categories:
   1. Provide a ***business continuity plan*** to provide assured operations for the protection of organizational intellectual property
   2. Provide a ***disaster recovery plan*** to provide assured operations for the protection of organizational intellectual property
   3. Provide an ***incident response plan*** to provide assured operations for the protection of organizational intellectual property
3. Select **one** of the Information Systems (IS) at the organization you’re focusing on, and develop **System Specific** assured operation plans for assured operations for: ***(a) the protection of organizational intellectual property, (b) implementation of access controls, as well as (c) patch and change management*** (CPM3). Ensure to separate the **System Specific** assured operation plans based on the following three categories:
   1. The ***protection of organizational intellectual property***
   2. The ***implementation of access controls*** including cyber-physical security controls
   3. ***Patch and change management***
4. Outline the strategic roles of the organizational stakeholders in planning and managing security, as well as providing assured operations as you’ve discussed above (CPM4). Ensure to separate the **discussion on roles of personnel in planning and managing security** based on the following key strategic roles:

* Board of Directors
* Senior Management
* Chief Information Security Officer (CISO)
* IT Management (CIO, IT Director, etc.)
* Functional Area Management
* Information Security personnel
* End users (employees, customers, sub-contractors/vendors, etc.)

1. Outline the anticipated top three to five biggest challenges that correspond to the implementation of contingency plans, System Specific assured operation plans and key strategic roles in the organizations.

**References**

You’re required to include at least **three** relevant references as you’re discussing the topic above. These must include:

* Recent (<2 years) industry white-paper or newspaper article
* US Government document (i.e. NIST, DHS, FBI, etc.)
* Peer-review journal article (<5 years)

**Requirement Summary**

* Your PowerPoint presentation file (about 12-15 slides, excluding cover slide and references) with the embedded audio of you presenting the slides.
* Your executive summary (3 to 4 pages) in Word document format addressing the key guidelines points above.
* Follow the assignment formatting requirements posted in Announcements in course Canvas.