7907ICT

Workshop Document

**This document is where you write-up the TEN weekly workshop tasks, each one of which is worth 10% of your total marks.**

# How to Approach these workshops (1 - 10)

This document lays out the ten workshop exercises to be completed each week. Either during the workshop session or at another time at your convenience. It contains detail of the task, plus a read-made template to be used when answering the questions.

This is the document that will be submitted for marking in two stages; Part A in week 6 to include workshops 1 through 5. Part B submitted in Week 11 to include weeks 6 to 10.

Key points to note:

* The output of each workshop is a **600-word written report**.
* Write your 600-word report into this workbook, accumulating them until you have completed all ten, then submit it via the Turnitin portal at the bottom of the assignment page of the course website.
* Don’t be tempted to leave doing the workshop write-up until the week the submission. It is a fact that we usually under-estimate the amount of work needed.
* As per university policy, extensions to the allowed time to submit can be granted with the necessary documentation. But please bear in mind that the IT industry is a very deadline driven profession.
* The workshops follow a similar format. Once you become familiar with the process, you should be able to work through the ten workshops over the duration of the course.
* The workshops can be completed individually or in discussions with groups of 2-4 students. Your submission will be an individual one, not a group submission.
* Ensure your report has clear headings for each.
* Try to do one workshop write-up per week.
* Avoid directly copying and pasting information from online sources, including generative language models like ChatGPT or other.

# Module 4: Assessing Incident Management Maturity

**<Workshop 4>**

### Introduction

Zenith Hospital is a regional healthcare provider which is expanding its business. However, as the business growing, they have become the target of hackers. Hackers have been trying to phish their staffs, though they have some protective measures for it but their staff awareness of the danger is still low. As an IT consultant company, we are ready to help Zenith assess their present circumstances with SEI's Incident Management Maturity Model and make an improvement plan for them.

### < SEI’s Incident Management Maturity Model >

The SEI's Incident Management Maturity Model (IMMM) is like a guide that helps companies figure out how good they are at dealing with unexpected incidents, like attack by hackers or viruses. It’s important because it let an organisation know their weakness then they can make improvement. Like many management modules, IAMMM assorts the capabilities of incident management into 5 categories, that is, Prepare, Protect, Detect, Respond, and Sustain, and each category can be divided into many subcategories to have more detailed information. What if the resources of an organisation for improving their response to incidents is limited? The IAMMM also classifies all categories into 3 levels of priority. For priority 1, the focus is on the essential capabilities that must be provided first, such as having a clear incident response plan, having a well interface for conducting incident management activities. For priority 2, capabilities are important that an organisation had better provide, such as an established IM information management plan. For priority 3, capabilities are additional to enhance operational effectiveness and quality.

#### < priorities>

In this scenario, Zenith Hospital should focus on building most critical incident management capabilities first. This includes developing a comprehensive and robust plan to respond to any case and training their staffs to have higher awareness of phishing attempts by hackers. Then, if extra resources are available, Zenith could improve detection systems, enhance communication for faster responses. These steps would make the hospital even more resilient against future cyber attacks.

#### <assessment>

For the Incident Management Function, the maturity level is initial as Zenith Hospital has basic incident response procedures, which means that they have started to establish an incident management function. However, the lack of a formalized incident response plan and the low level of staff awareness suggest that this function needs to be more completed. The maturity level of Threat and Vulnerability Management is managed. The recent increase in phishing attempts points to gaps in Zenith’s ability to manage threats and vulnerabilities effectively. It suggests that while there may be some measures in place to address these issues, such as basic antivirus software or firewalls, they are not sufficient to handle the evolving nature of cyber threats. The hospital likely lacks a systematic approach to identifying, assessing, and mitigating vulnerabilities. Lastly, the maturity level of situational awareness is initial. The low staff awareness of cyber threats, combined with the reactive nature of the current incident response procedures, indicates that Zenith’s situational awareness is minimal. This means that the hospital may not have the necessary tools or processes in place to continuously monitor its environment for potential threats. Without adequate situational awareness, the hospital cannot effectively anticipate or respond to incidents.

#### <roadmap>

To improve its incident management, Zenith Hospital should start by creating a clear response plan, training staff, and setting up a team to handle incidents. They should also begin checking for security weaknesses and gathering information on potential threats. Over the next few months, they should practice their response plan, upgrade their threat detection tools, and improve how they monitor for risks. By the end of the year, the hospital should have advanced tools in place, a strong program for managing vulnerabilities, and ongoing training to keep staff prepared and aware. This step-by-step approach will help the hospital become better at handling incidents.

### Conclusion

Zenith Hospital can significantly enhance its incident management capabilities. Focusing on foundational improvements in planning, staff training, threat detection, and situational awareness will build resilience against cyber threats, ensuring better protection of patient data and continuity of critical services.

### References

<Use APA referencing style>

<References not included in wordcount>