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, … For priority 2…. For priority 3…

#### < priorities>

#### <assessment>

#### <roadmap>

### Conclusion

### References

<Use APA referencing style>

<References not included in wordcount>