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 1: Evaluating IT Governance Frameworks

**<Evaluate IT Governance Frameworks>**

### Introduction

As a CISO, my primary job is to implement cybersecurity in our company, especially our services are finance-related, it could involve in a huge amount of funding, so we should bring the security level to a higher level than other normal companies. The spirit of cybersecurity is protection and prevention, in other words, the main task for me is to make sure that the data in our company is safe and our operation is aligned with the regulations and laws. Furthermore, I should find out the vulnerability of our system or services and fix it before it is exposed to potentially attackers. Based on my knowledge, I will analyse the issues our company has encountered recently and select an IT government framework (or multiple) to address these troubles.

### <IT GoverNMENT FRAMEWORKS>

COBIT and ITIL are the two most popular IT government frameworks in this industry, while it’s difficult to select between COBIT, ITIL or combination of these two frameworks. As a junior CISO, I don’t have much experience and we only have limited resources to deal with these issues. Furthermore, I want the process to be as simple as possible and the troubles can be solved in a very short time, so I would choose ITIL framework as the final resolution. The reason I don’t choose COBIT is that it is a comprehensive framework which covers 37 processes so it may take much time to understand the details and deploy it. So as combination of two frameworks, I don’t want to make it too complicated so that I can fix the issues as fast as possible. In the following, I am going to analyse the pros and cons of the framework I select – ITIL.

#### <ITIL>

ITIL is a comprehensive framework dedicated to aligning IT services with business goals and customer needs by providing reliable IT services (Axelos, 2019). One of the key principles of ITIL is “focus on values”, which ensures that the purpose of management is to deliver better services to customers and elevate customer satisfaction. Another core component of ITIL is continuous improvement by collecting feedback, learning from mistakes and making changes, it could form a good culture in our organisation and bring our services to the next level.

#### <Challenges>

Based on what I know about these IT government frameworks, I think there is no one framework can completely be applied to any organisation. When it comes to implementation, it is necessary to customise some of the content to fit the specific context, like I said, I am a junior CISO, so I might need a consultant to discuss with the really detailed process to implement this framework. Another challenge we may have is that as our business growing, we may need a framework encompassing a broader range of IT management, like COBIT, so we may need extra cost to transform our framework by the time.

### Conclusion

In summary, as a junior CISO, my main job is to keep our company’s data safe, especially since we handle finance-related services. I have chosen to use the ITIL framework because it’s straightforward and aligns well with our business needs, helping us improve our IT services quick. While ITIL is effective, it might need some adjustments to fit our specific situation, and as we grow, we may need to explore more comprehensive options like COBIT (ISACA, 2012). For now, keeping things simple and focusing on immediate improvements is our best strategy.

### References

Axelos (2019a). *ITIL ® Foundation ITIL 4 Edition*. Norwich: Tso.

Information Systems Audit And Control Association (2012a). *COBIT 5 : enabling processes.* Rolling Meadows, Ill.: Isaca.

# Module 2: Developing an Ethical Hacking Policy

**<** **Developing a Comprehensive Ethical Hacking Policy>**

### Introduction

As a CISO, I should ensure that the cybersecurity in our system is at highest level as we are a financial company, any accident, invasion or data breach may cause serious consequence and huge amount of money. So, I would like to develop an ethical hacking program to find out the vulnerabilities in our system and fix it before the potential attackers know it. However, there are some risks and challenge in implementing such an ethical hacking practice, so I must make a very detailed blueprint to avoid any accident as much as possible.

### <scope and objective>

The aim of this ethical hacking program is to find the defects and test the resilience of our systems. Thus, anything that is not related to our goal should be excluded as we should lower the risk as much as possible. Specifically, we want to check our access control and identity management to ensure that only the person who is authorized can access our system. Furthermore, operating systems security, network security and database security are also included in this project. According to Harris (2019), the continuous evaluation of these components is crucial in maintaining a robust security posture, especially in financial institutions where the stakes are exceptionally high.

#### <Roles and responsibilities>

There are many roles in our information security office. In this program, we will assign roles such as penetration testers, who will try to hack in our system with permission and must follow the policies in the whole process, a program director, who will supervise the activities and respond to superior officer, and a cybersecurity consultant, who has rich experience in the field and will provide us advice for improvement. There are some other roles outside of our information security office, such as legal team, we will consult with them to ensure that our activities are fully aligned with the related laws and regulations.

#### <Implement process>

In the initial step, we have to draft a consent and authorization document which should include the scope and purpose of this program, responsibilities, and legal compliance, then submit it to the related department for approval. After getting approval, we can start our program. Our ethical hackers are going to use their techniques and knowledge to invade our system through all potentially vulnerabilities we might have such as WIFI network, devices with Bluetooth, control panel password, fishing email or even by social engineering. In this step, our respond team will be standing by, if an incident happens, they will start the plan we have made for remedy, like shutting down our power to terminate the hacking activity, notifying related stakeholders and superior officers. This process will be lasting for 30 days, 24/7, without any break. We design it in this way because the real hackers always hack in your computer or system at unexpected time and with creative approaches. Hence, I think it’s a good practice to set limit as less as possible for real-life scenarios.

#### <Reporting>

After the hacking activity, we will list all the vulnerabilities founded in this program and analyse it with our cybersecurity consultants to find out the reasons and improve it. At the same time, I will audit and inspect the record of the whole process to make sure all our activities comply with the policies, terms and regulations. Then, we will summarise the report and send it to the CEO.

### Conclusion

This ethical hacking program it to help our organisation prevent the potential invasion of our system in the future. As I said in the beginning, we are a financial institute, so a cybersecurity incident could cause huge loss, millions, billions of dollars, or even more. It’s impossible to make any physical or virtual system absolutely safe, because the technology evolves every year, or maybe faster. For example, in the field of Cryptography, it’s nearly impossible to crack a 20 digits password encrypting in SHA-512 with brute-force attack approach, as the time it requires for computing is way longer than the earth lifespan. But as the rapid development of Semiconductor industries, the computility of GPU and CPU grows exponentially, so it’s hard to say these encryption methods we apply these days will still be safe after 10 years. However, we don’t need to be too worried about it, as long as we keep the core spirit of cybersecurity, that is, continuous improvement, I believe the justice parties will always win in the end.

### References

MaymíF. and Harris, S. (2022). *All in one CISSP exam guide.* New York: Mcgraw-Hill Education.

# Module 3: Data Breach Response Plan

**<DATA BREACH RESPONSE PLAN>**

### Introduction

In today’s digital world, responding to data breaches is crucial for any organization. This workshop lets me apply the concepts from Module 3 by Identifying the key roles and responsibilities and developing a data breach response plan for CyberTech.

### <Key roles and responsibilities>

A data breach response team requires agility very much so that we can mitigate the loss of data breach incident. We have a team leader, who is responsible for leading the team, integrating ideas, assigning tasks and reporting to senior management. Two Risk management supports, whose job is to assess the risks from the breach. A Legal support, who is in charge of identifying regulations and laws related to us. 3-5 IT supports, they are responsible for establishing the cause and impact of a data breach that involved ICT systems, recovering data and making sure our system is secure.

#### <response>

A data breach response team should develop various SOPs for incidents in different scenarios so that we can respond to the incidents as fast as possible. In general, it’s a good practice to follow these 4 steps to respond to a data breach incident, that is, contain, assess, notify and review. The purpose of contain process is to prevent the scale-up of the harm that is made already, like when we are bleeding, we always keep pressure on our wound to stop bleeding so that we can avoid the risks caused by excessive bleeding. In this step, we can shut down the system and revoke most computer access privileges to cease the on-going data breach process. Second step is assess, it helps us identify the risks and find solutions for it. In this step we have to evaluate the risks and impact by collecting detailed information, then we could have a clear understanding of how it happens and the potential harm which could affect our system, organisation or customers. Next step is notify, it’s necessary to notify related stakeholders about the data breaches so that they can take some actions to protect themselves, for example, they can change their password and apply multi-factor authentication to prevent the potential breaches in the future. The final step is to review, this is a critical step as if we don’t examine our vulnerabilities and fix it, then it might happen again and again which is not a good practice. In this step, we have to analyse the incident thoroughly and product a report and develop a prevention plan to avoid data breaches incidents in the further (Cichonski et al., 2012)

#### <OAIC>

OAIC stands for Office of the Australian Information Commissioner, which is responsible for legislating privacy regulation and information policies and providing data protection guidelines to organization (OAIC, 2023). When serious data breach incidents happen, including unauthorized access into database or disclosure of personal information, we should notify OAIC as soon as possible. In some cases, we should notify some third parties as well, such as related bank, financial institutions, educational institutions or hospitals. It could help the harm keep scaling-up.

#### <Other actions>

In the discussion above, we ignore the human factors in this scenario, while acknowledging that human error and behaviours play a critical role in both the occurrence and response to data breaches. Thus, if we have additional resources, we may use it to train our employees so that we can reduce the probability of data breach caused by individuals.

### Conclusion

Having a solid data breach response plan is vital for any organization today. By setting clear roles and following a simple 4-step process - contain, assess, notify, and review. CyberTech can quickly manage and reduce the impact of data breaches. It's also important to follow legal guidelines and notify the right authorities when needed. Finally, training employees can help prevent breaches caused by human mistakes. By doing all this, CyberTech can better protect its data and keep everyone safe.

### References

Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012). Computer security incident handling guide. *Computer Security Incident Handling Guide*, [online] 2(2). doi:https://doi.org/10.6028/nist.sp.800-61r2.

OAIC (2023). *Data breach preparation and response*. [online] OAIC. Available at: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response.

# Module 4: Assessing Incident Management Maturity

**<** **ASSESSING INCIDENT MANAGEMENT MATURITY>**

### 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

# Module 5: Ethical AI Case Study Analysis

**<Ethics in IT Industry>**

### Introduction

A leading AI company called TechnoCore is facing some troubles, their hiring system has been found that existing an unfair mechanism to select candidates, such as woman, minorities and non-traditional paths people have less opportunity to get an interview.

### <ETHICS in enterprise>

Enterprises always put the profit as their priority, there is nothing wrong with that. But a great enterprise should also consider ethics and responsibilities to society. Laws and regulations are the lowest standards of ethics, serving as the basic rules that all companies must follow. With higher standards of ethics, most of times, enterprise could not have direct benefit, but for long-term view, it could promote the development of society and get positive feedback then form a positive cycle finally.

#### <Ethical Issues>

TechnoCore faced some big troubles with fairness when they used their job application filter system to help pick people for interviews. The system was only choosing people who looked like the ones it was trained to recognize, which were mostly men from certain schools and women are always ignored. This meant it was leaving out lots of good people who didn't fit that narrow group, like women and people from different backgrounds. The problem was that the system wasn't fair, and it wasn't transparent to see how it was making its choices. Because of this, TechnoCore needed to figure out how to make sure everyone had a fair chance to be chosen. This issue highlights the broader ethical concern that AI systems, if not properly designed and monitored, can reinforce existing biases and inequalities (Binns, 2017)

#### <priorities>

The most important thing for TechnoCore is to make sure their hiring process is fair by fixing the filter system that was unfairly leaving people out because of their gender, race, or education background. They need to stop this unfairness so that everyone can get a fair chance. It’s also important that TechnoCore explains how the system makes its choices and takes responsibility if it makes mistakes. Lastly, they should focus on bringing in different kinds of people to make their company more diverse and more creative.

#### <SOLUTIONS>

To solve the problems TechnoCore is facing, we should know what cause the system to have these biased choices. Maybe it’s because the amount of data for training is not enough, or the quality of the data is not good, then they can consider re-training the model in the filter system. And they should also have people regularly review and audit the system’s decisions to catch any mistake in real time. In other hand, TechnoCore should be open about how the system works and be ready to make changes if needed. For example, making the system open-source is a good practice. As Cathy O'Neil (2016) discusses in *Weapons of Math Destruction*, the dangers of opaque algorithms in decision-making processes can lead to significant social harm if not properly managed.

### Conclusion

Being ethical is vital for companies, no matter what products or services that a company sells, no matter how good quality it is, in the end they are just selling trustiness. Honest, transparent, fairness, integrity and accountability, all these ethics are not necessary to build a company, but if you want to develop a long-term business then they are bloody important. Thus, TechnoCore needs to fix their hiring system to make sure it’s fair to everyone. By being honest about how the system works and making sure it doesn’t unfairly leave people out, they can create a better and more diverse workplace. Doing this will help them not only do the right thing but also make the company stronger and more successful in the long run.

### References

Binns, R. (2017). *Fairness in Machine Learning*.

O’Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.