7907ICT MODULE WORKSHOPS

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 FOR YOUR ORGANIZATION

Scenario: You are the Chief Information Security Officer (CISO) of a medium-sized financial services company. The company has recently experienced some security incidents, compliance issues, and customer complaints related to its IT operations. The CEO has tasked you with evaluating and recommending an appropriate IT governance framework to improve the management and oversight of the company's IT resources and processes.

Instructions:

1. Review the key concepts and examples of IT governance frameworks covered in Module 1, such as COBIT, ITIL, ISO/IEC 38500, and AS8015-2005.
2. Analyse the current state of your organization's IT governance practices, considering factors such as:
    - Alignment of IT with business objectives
    - Management of IT risks and compliance
    - Delivery and performance of IT services
    - Roles and responsibilities for IT decision-making
    - Monitoring and reporting of IT operations
3. Identify the specific challenges or areas for improvement in your organization's IT governance.
4. Based on the analysis, select the IT governance framework (or combination of frameworks) that would be most suitable for addressing your organization's needs and challenges.
5. Provide a written answer (approximately 600 words) that includes the following:
    - A brief overview of your organization's current IT governance state and challenges
    - The IT governance framework(s) you have chosen and the rationale for your selection
    - The key principles, processes, or components of the selected framework(s) that will address your organization's specific needs
    - The potential benefits and challenges of implementing the selected framework(s)
    - A high-level plan or roadmap for adopting and implementing the selected framework(s) in your organization

This exercise will help you understand and apply the concepts of IT governance frameworks, analyse organizational needs and challenges, evaluate different framework options, and develop a practical plan for implementing an IT governance framework in your organization.

MODULE 2: DEVELOPING AN ETHICAL HACKING POLICY

Scenario: You are the Chief Information Security Officer (CISO) of a large financial institution. Your organization is considering implementing an ethical hacking program to strengthen its cybersecurity posture and identify potential vulnerabilities in its systems and networks. However, you are aware of the legal and reputational risks associated with ethical hacking activities, and you want to ensure that your organization follows best practices and ethical principles.

Instructions:

1. Review the key concepts and guidelines discussed in Module 2 related to ethical hacking, such as responsible hacking practices, mitigating legal and reputational risks, and the role of ethical hacking in cybersecurity.
2. Consider the specific risks and challenges your organization might face when conducting ethical hacking activities, considering factors such as the sensitivity of financial data, regulatory compliance requirements, and the potential impact on the organization's reputation and customer trust.
3. Develop a comprehensive ethical hacking policy that outlines the principles, procedures, and controls your organization will adopt to ensure that ethical hacking activities are conducted responsibly, ethically, and in compliance with legal and regulatory requirements.
4. Your ethical hacking policy should address the following elements (approximately 600 words):
    - The scope and objectives of the ethical hacking program
    - The roles and responsibilities of the ethical hacking team and other stakeholders
    - The process for obtaining consent and authorizations from relevant parties
    - The guidelines for conducting ethical hacking activities, including the tools and techniques to be used
    - The reporting and communication procedures for sharing findings and recommendations
    - The measures to protect sensitive data and maintain confidentiality
    - The mechanisms for monitoring and auditing ethical hacking activities
    - The procedures for addressing legal and regulatory compliance requirements
    - The provisions for training and awareness programs on ethical hacking practices
    - The strategies for mitigating legal and reputational risks associated with ethical hacking

This exercise will help you understand the importance of ethical hacking in cybersecurity, while also developing practical skills in creating policies and guidelines that balance security needs with legal and ethical considerations.

MODULE 3: DATA BREACH RESPONSE PLAN

In this exercise, you will work in small groups or individually to develop a data breach response plan for a fictional company.

Company Background:

CyberTech Solutions is a medium-sized IT consulting firm with 150 employees. They provide cybersecurity services like penetration testing, security audits, and incident response to clients across various industries. CyberTech handles sensitive client data including network diagrams, vulnerability reports, and some personal information of client employees.

Tasks:

1. Identify the key roles and responsibilities that should be part of CyberTech's data breach response team. Assign team member roles to your group.
2. Outline the 4 main steps CyberTech should take when responding to a data breach (contain, assess, notify, review). For each step, specify 2-3 key actions the response team should carry out.
3. Determine when CyberTech would need to notify the OAIC, affected individuals, and other third parties about a data breach under the Notifiable Data Breaches scheme.
4. Discuss additional sections or information that should be included in CyberTech's comprehensive data breach response plan.

Output:

Each group should prepare a maximum 600-word written summary outlining their data breach response plan for CyberTech Solutions. The summary should cover the main points addressed in the tasks above.

This exercise allows you to apply the concepts from Module 3 by developing a practical data breach response plan. It covers key elements like the response team, core response steps, notification requirements, and plan documentation. You will reinforce your understanding through discussion and collaborative work.

MODULE 4: ASSESSING INCIDENT MANAGEMENT MATURITY

Objective:

To understand the key components of the SEI's *Incident Management Maturity Model* and apply it to assess the maturity level of an organization's incident management capabilities.

Scenario:

Imagine Zenith Hospital, a regional healthcare provider with a growing network of clinics. They've recently experienced a surge in phishing attempts targeting staff. While IT has basic incident response procedures, staff awareness of cyber threats seems low. This scenario presents a challenge – how mature is Zenith's incident management, and what improvements are crucial to protect sensitive patient data and ensure business continuity in case of a cyberattack?

Your team, assigned Zenith Hospital, will utilize the SEI's Incident Management Maturity Model to assess their current state and develop a roadmap for improvement. Focus on prioritizing capabilities critical for healthcare, like incident identification, communication, and recovery. Remember, a robust incident management plan is vital to safeguarding patient privacy and mitigating disruption to critical medical services.

Instructions:

1. Divide the class into small groups of 3-4 students. Or work individually.
2. Use the provided scenario.
3. Using the information provided in the module notes, particularly the list of capabilities and their priorities, each group should:
    a. Identify the incident management capabilities their assigned organization should prioritize based on the organization's nature and potential risks.
    b. Assess the organization's maturity level for each of the prioritized capabilities, considering the indicators and scoring criteria provided in the notes.
    c. Develop a roadmap or action plan for improving the organization's incident management maturity, focusing on the highest priority capabilities that need improvement.
4. After 20 minutes of group work, each group will present their findings and proposed roadmap for 5 minutes.

Expected Output:

Each group should submit a written report (approximately 600 words) that includes:

1. A brief description of the assigned organization scenario.

2. A list of the prioritized incident management capabilities for the organization, with justifications.
3. An assessment of the organization's current maturity level for each prioritized capability, supported by evidence from the module notes.
4. A proposed roadmap or action plan for improving the organization's incident management maturity, with recommendations for addressing the identified areas for improvement.

This exercise will help you understand the practical application of the SEI's Incident Management Maturity Model, reinforce your knowledge of the different incident management capabilities, and develop skills in assessing an organization's maturity level and proposing improvement strategies.

MODULE 5: ETHICAL AI CASE STUDY ANALYSIS

Work in small groups or individually to analyse an ethical case study involving the use of AI technology. The goal is to apply the ethical decision-making models, principles, and considerations covered in the module notes.

Scenario:

TechnoCore, a leading AI company, developed a resume screening system using machine learning to help streamline their hiring process. After deploying the system, they noticed a sharp decline in candidates from underrepresented backgrounds like women, minorities, and non-traditional education paths making it through to interviews.

An internal audit revealed the training data was heavily biased towards resumes from elite universities and technological fields dominated by young, white males. The system was treating attributes like ethnic names, gender-coded language, and lack of prestigious credentials as negative signals, perpetuating historical biases.

TechnoCore now faces a dilemma - keep using the cost-saving system despite its ethical issues or find an alternative that promotes equitable hiring but may be more resource-intensive. As an ethical AI governance board, how should they proceed?

Instructions:

- Using the provided scenario, read through the case study assigned to your group (5 minutes)
- As a group, or individually, identify the key ethical issues and stakeholders involved using the guidelines from section 5.4 Ethical Decision Model (10 minutes)
- Prioritize the issues and stakeholder impacts based on the ethical theories, principles and values discussed in sections 5.3, 5.5 and 5.6 (5 minutes)
- Propose potential solutions or mitigation strategies to address the ethical concerns, referring to the recommendations in 5.6 on AI bias mitigation (5 minutes)
- Each group will have 5 minutes to present their case analysis and proposed solutions to the class.

Output:

After all group presentations, individually write up a 600 word analysis of your group's case study that covers:

1. The key ethical issues identified
2. The prioritization of issues based on ethical principles
3. Your recommended solution and rationale for why it is ethically justified

This exercise will allow you to apply the ethical decision-making framework, moral philosophies, and AI ethics guidelines from the module in a practical context. Be prepared to discuss, debate and justify your ethical reasoning with examples from the notes.

MODULE 6: THE ETHICS OF OPEN-SOURCE SOFTWARE LICENSING

Duration: 30 minutes

Objective: This exercise aims to reinforce the main ideas and ethical considerations around open-source software (OSS) licensing, as discussed in the module notes. The exercise will encourage you to critically analyse the implications of different OSS licenses and develop a well-reasoned position on how to address ethical dilemmas that may arise from the use of OSS.

Instructions:

1. Divide the class into small groups of 3-5 students.
2. Assign each group one of the following scenarios:

Scenario A: You are a developer who has created a powerful data analysis tool using various OSS libraries. Your tool has the potential to be used for both beneficial and harmful purposes, such as targeted advertising or surveillance. You want to release your tool under an OSS license but are unsure which license to choose.

1. Within your groups, you should discuss the following questions:
   - What are the ethical considerations and potential risks associated with the given scenario?
   - Which OSS license(s) would be most appropriate for the scenario, and why?
   - What steps or measures can be taken to mitigate the identified ethical risks?
   - How would you balance the various interests and perspectives of different stakeholders (e.g., developers, users, companies, governments, advocacy groups)?
2. After 20 minutes of discussion, each group should prepare a 600-word written response summarizing their analysis and recommendations.
3. In the remaining 10 minutes, each group should present their response to the class, and the instructor should facilitate a broader discussion on the ethical implications of OSS licensing.

Evaluation:

The written responses and group presentations will be evaluated based on the following criteria:

- Identification and analysis of relevant ethical considerations and risks
- Justification and rationale for the chosen OSS license(s)
- Proposed measures to mitigate ethical risks and address stakeholder interests
- Clarity, coherence, and persuasiveness of the arguments presented

This exercise will encourage you to critically think about the ethical implications of OSS licensing, consider different perspectives and interests, and develop a well-reasoned position on how to address potential ethical dilemmas. The group discussions and written responses will reinforce the main ideas covered in the module notes while also fostering collaboration, communication, and decision-making skills.

MODULE 7: CYBER FORENSICS AND INTELLIGENCE ANALYSIS

Instructions:

Imagine you are a cybersecurity consultant hired by a company that recently experienced a data breach. Your task is to conduct a cyber forensics investigation and gather threat intelligence to understand the nature of the breach and the potential actors involved.

1. Cyber Forensics Investigation (15 minutes):

- Outline the key steps you would follow in conducting a cyber forensics investigation, considering the legal aspects and admissibility of evidence.
- Describe the different stages of the forensics process, from readiness and evaluation to collection, analysis, presentation, and review.
- Discuss the potential countermeasures that criminals might employ to obfuscate or conceal their activities, and how you would address them.

2. Threat Intelligence Analysis (15 minutes):

- Identify at least three primary sources of cyber intelligence (e.g., SIGINT, OSINT, TECHINT) that you would leverage to gather information about the potential threat actors and their tactics, techniques, and procedures (TTPs).
- Explain how you would establish a Cyberthreat Intelligence Program (CIP) within the company, considering the operational and strategic components.
- Discuss the importance of collaborating with external entities, such as information sharing and analysis centres (ISACs) and threat intelligence communities, in gathering and sharing relevant threat intelligence.

Output:

After completing the exercise, you should provide a written answer of approximately 600 words, addressing the following:

1. A summary of the cyber forensics investigation process, highlighting the legal considerations and admissibility of evidence.
2. An overview of the threat intelligence sources and methods they would employ to gather information about the potential threat actors and their TTPs.

3. A brief outline of how they would establish a Cyberthreat Intelligence Program (CIP) within the company, including operational and strategic components, as well as external collaborations.

This exercise aims to reinforce the concepts of cyber forensics, threat intelligence gathering, and the establishment of a Cyberthreat Intelligence Program (CIP). It encourages you to think critically about the practical application of these concepts in a simulated scenario, while also considering legal aspects and collaboration with external entities.

MODULE 8: ETHICAL AND INCLUSIVE TECHNOLOGY FOR SOCIAL GOOD

Imagine you are a consultant hired by a technology company that aims to develop innovative solutions to address social and environmental challenges. Your task is to propose a framework for ensuring that the company's products and services are designed and implemented ethically, inclusively, and with a positive social impact.

1. Ethical Innovation and Social Impact (10 minutes):

- Identify a specific social or environmental problem that the company could address using technology (e.g., education, healthcare, sustainability, human rights).
- Define the purpose, vision, and desired impact of the proposed technology solution.
- Outline the key ethical principles and standards that should guide the development and implementation of the solution.

2. Accessibility and Inclusivity (10 minutes):

- Discuss the importance of accessibility and inclusivity in the context of the proposed technology solution.
- Identify potential barriers or challenges to accessibility and inclusivity that should be addressed (e.g., digital divide, disability, cultural diversity).
- Suggest strategies and best practices for promoting accessibility and inclusivity throughout the product lifecycle.

3. Stakeholder Engagement and Ethical Decision-Making (10 minutes):

- Identify the key stakeholders (e.g., users, beneficiaries, communities, partners, regulators) that should be involved in the development and implementation of the proposed technology solution.
- Discuss the potential ethical dilemmas or conflicts of interest that may arise among stakeholders, and how these could be addressed through ethical decision-making processes.
- Propose mechanisms for ongoing stakeholder engagement, feedback, and accountability to ensure the solution remains aligned with ethical principles and social values.

Output:

After completing the exercise, you should provide a written answer of approximately 600 words, addressing the following:

1. A brief overview of the proposed technology solution, its purpose, and desired social impact.
2. The ethical principles and standards that should guide the development and implementation of the solution.
3. Strategies for promoting accessibility and inclusivity throughout the product lifecycle.
4. Approaches for stakeholder engagement, ethical decision-making, and ongoing accountability to ensure the solution remains ethical and socially responsible.

This exercise aims to reinforce the concepts of ethical innovation, accessibility, inclusivity, and stakeholder engagement in the context of developing technology solutions for social good. It encourages you to think critically about the potential challenges and dilemmas that may arise, and to propose practical strategies and frameworks for addressing them.

MODULE 9: ASSESSING CYBER RISK AND INSURANCE NEEDS

Instructions (Time: 30 minutes)

1. Spend 5 minutes reading through the case study section on the WannaCry ransomware attack (Section 9.3).
2. Divide into small groups of 3-4 students or work individually.
3. Imagine you are the cybersecurity team for a medium-sized manufacturing company with operations in multiple countries. Your assignment is to assess the potential cyber risks your company faces related to ransomware and malware attacks like WannaCry.
4. As a group, spend 10 minutes discussing and listing out the major cyber risks and potential impacts a ransomware/malware incident could have on your manufacturing operations, supply chain, customer data, financials, reputation etc.
5. Next, spend 10 minutes evaluating what cybersecurity controls, processes and insurance coverage your company should have in place to mitigate and transfer these risks. Consider technical controls, incident response plans, cybersecurity awareness training, cyber insurance policy types and coverages etc.
6. Select one member from your group to summarize your findings in a 5 minute presentation covering:
   - The top 3 cyber risks identified
   - The cybersecurity program elements recommended to mitigate them
   - Potential cyber insurance coverage needs
7. Each group will give their 5 minute presentation summarizing their assessment.

Written Answer (Length: ~600 words)

For the written answer, select one of the cyber risks your group identified related to ransomware/malware and explain in more detail:

1. The nature of this risk and potential impacts to the business
2. Specific cybersecurity controls to prevent/mitigate this risk
3. How cyber insurance could help transfer residual risk after controls
4. Any other key considerations regarding this cyber risk

This exercise reinforces understanding of modern malware threats like WannaCry, the cyber risk management process, core cybersecurity program elements, and the role of cyber insurance. It promotes applying concepts from the module notes to a realistic business scenario through group discussion and presentations.

MODULE 10: BALANCING PRIVACY AND SECURITY IN REMOTE WORK POLICIES

Instructions: Duration: 30 minutes

1. Divide the class into small groups of 4-5 students.

2. Assign each group the role of a cybersecurity governance team working for a government agency or a large corporation.

3. Provide the following scenario:

Your organization has recently adopted a remote work policy to promote flexibility and work-life balance for employees. However, concerns have been raised about the potential risks to data privacy and security when employees access sensitive information from home or public locations.

Your team's task is to develop a set of guidelines and recommendations for a comprehensive remote work policy that addresses these concerns while respecting employees' rights to privacy and autonomy.

4. Each group should consider the following aspects and incorporate them into their recommendations:

- Data security measures (encryption, VPNs, access controls)
- Employee privacy rights and consent
- Monitoring and surveillance practices
- Handling and sharing of sensitive information
- Acceptable use of personal devices and public networks
- Training and awareness programs
- Compliance with relevant laws and regulations (e.g., Privacy Act, GDPR)
- Balancing organizational needs with individual privacy

5. After 20 minutes of discussion and brainstorming, each group should prepare a 600-word written answer outlining their recommendations for the remote work policy.

6. Groups can then take turns presenting their recommendations to the class, followed by a brief Q&A session.

7. Encourage you to provide constructive feedback and share your perspectives on the challenges and trade-offs involved in balancing privacy and security in remote work environments.

This exercise reinforces the main ideas from Module 10 by allowing you to apply your knowledge of e-government, digital transformation, data privacy, security, and ethical considerations to a practical scenario. It will also promote critical thinking, collaboration, and communication skills essential for cybersecurity governance professionals.

NOTES