Information Security Formulation & Implementation
Final examination
2 Hours

A. This examination consists of questions on material taught through the lecture sessions and associated references.
   - **Part A** (20 Marks - 20%) has ten (15) multiple-choice questions;
   - **Part B** (80 Marks – 80%) has six (8) questions that require detailed, complete and correct answers. Be concise with your answers by using the fewest words possible to provide detailed, complete and correct answers.

B. You are required to provide detailed, complete and correct answers to the questions

C. You must work individually. The order of questions does not correspond with the order of the course material, associated difficulty or importance.

D. This is a closed book examination and no reference materials are allowed in the examination room. No books, no course notes or printouts of any kind. No calculators, no cellphones/smartphones, computers, or electronic devices of any kind. You must turn off any electronic devices and store them under your desk simply having any device (even if turned off) with you during the exam constitutes a violation and will be reported. If you need to borrow a pencil, sharpener, eraser, etc., you must ask a proctor. You are not allowed to directly talk to any of your neighbours in the examination room.

E. Before, during, and at the end of the examination:
   - You are not allowed to leave the examination room during the examination room period, except for visits to the washrooms.
   - Please do not stand up or talk until all examinations are is picked up; this also applies to cases where you finish earlier than the allotted period.
   - Ask the proctor questions that are meaningful in the context of the examination. Ensure that your questions are not probing for answers to the examination questions.
   - If you are found cheating, involved in discussions, talking to other students or causing any kind of disturbance during the examination, then you will be reported to appropriate University officials for violation of examination policy; you will face appropriate sanctions according to the university examination policy.
   - Answers must be properly marked in the answer book with the corresponding question number. Only answers in the answer book will be marked and graded.
   - Return both the answer/question books back to the proctor before leaving the examination hall.
   - You must stop writing when any of the proctors announces that the allotted examination duration has expired.

Part A – Multiple Choice Questions - 20 Marks (Overall 20%)

1. An information security policy is a primary requirement for protecting information assets in an organization. Which of the following is not a reason why this is the case?
   A. A policy establishes the authority and accountability to protect the organization's assets.
   B. The policy provides the mandate for implementing an information security programme.
   C. A policy establishes the steps required to put security in place.
   D. A policy sets the expectations for the employee's behaviour regarding security.

2. One of the following statements is true regarding security policy. It …
   A. enables management to define IT system access rules.
   B. provides a way to identify and clarify security goals and objectives.
   C. helps establish a cost model for security activities.
   D. is a means to allow management to define system recovery requirements.

3. The following are good policy guidelines regarding information security in an organization except:
   A. Developed using industry-accepted practices.
   B. Formally agreed to by act and approved by law enforcement.
   C. Distributed using all appropriate methods to all concerned.
   D. Reviewed, read and understood by all employees.

4. In developing relevant and hence effective policies, it is essential to conduct a risk assessment. Why?
   A. The law, standards and regulations require that organizations conduct risk assessment as the basis of policy development.
   B. A risk assessment will determine the risks to be mitigated and how they relate to the organization's strategic objectives.
   C. Security policies are controls that mitigate risks identified during the risk assessment phase of policy development.
   D. To achieve its strategic objectives the organization must conduct a risk assessment.

5. The statement 'policies are a countermeasure to protect assets from threats' is supported by all of the following statements except:

   A. They exist to inform stakeholders of acceptable behaviour.

   B. Are intended to enhance employee productivity and deter potentially harmful circumstances.

   C. Are automated means of enforcement of desirable employee conduct.

   D. Explicitly state the consequences of failure to comply.

6. Organizations use information security governance documents of policies, standards, guidelines and procedures for effective information security management. In this context, which of the statements below accurately represents the term 'standards'?

   A. Standards represent the first elements defined in an effective security policy regime.

   B. Standards represent senior management's high-level statements in support of an entity's information security programme.

   C. Standards are senior management's directives to create a computer security programme.

   D. Standards are defined after policies have been enunciated and describe how policies will be applied within an entity.

7. Comprehensive security education, training and awareness programmes are important for effectively enforcing information security policies. A key purpose of such programmes includes:

   A. Developing key needed skills to strengthen the organization's information security programme and enhance the chances of its success.

   B. Building in-depth knowledge in information security at the organization.

   C. Improving awareness of purpose, scope and accountabilities relating to specific policies.

   D. Pronouncing required access control routines and processes for specific assets in an organization.

8. Which of the following is NOT a performance measure organizations use concerning information security?

   A. The evaluation of the compliance of non-security personnel in adhering to the information security policy.

   B. The effectiveness of the implementation of an information security policy.

C. The assessment of the impact of incidents or other security events on the organization or its mission.

D. The determination of the effectiveness and/or efficiency of the delivery of information security services.

9. One of the following is not among the properties of a well-structured policy:

A. Has clearly stated purposes and objectives.

B. Has plainly defined terms to ensure there is no ambiguity.

C. Is reviewed at a fixed time defined in the policy, albeit regularly.

D. Developed based on a clear risk assessment methodology.

10. Intellectual property (IP) policies are essential in organizations for, among others, one of the reasons:

A. IP rights are intended to benefit end users and help cultivate the market for inventors, artists, scientists and businesses for their investment in effort, time, money, etc. into their works.

B. IP fuels progress – new ideas and creations. Technological advancement depends on continuous development and application of new inventions;

C. IP protection limits the ability of IP owners to trade, lease or license their IP like any other property.

D. IP laws overly favour the creative class at the expense of the end user's rights to access the proceeds of humanity's creativity.

11. Policy compliance is a means of assuring that those policies, once implemented, are adhered to. Policy compliance includes all of the following, except:

A. Performance measures (metrics/indicators) to gauge the degree to which the policy is complied with.

B. Mandatory compliance audits to ensure that policies are adhered to.

C. Responsibility/accountability for assessing compliance.

D. Related processes and procedures for assessing compliance, including the data to be collected.

12. Organizations conduct elaborate education, training and awareness programmes. A primary goal of such a programme is:

A. The programmes are vehicles for communicating required security procedures in the organization.

B. These programmes offer a chance to disclose and discuss the organization's exposure and the related risk analysis.
C. Such programmes provide a clear appreciation of potential risks and exposure to the organization's information assets.
D. The programmes are typically used to communicate user responsibilities.

13. There is a distinction between knowledge-based and behaviour-based metrics for information security compliance measurement. All of the following, except one, are examples of knowledge-based metrics.

A. The proportion of employees who have passed the mandatory policy-based quiz.
B. The frequency and total number of awareness courses conducted in a year.
C. The percentage of employees who have complied with password policies.
D. The proportion of employees who have attended awareness training.

14. An effective information security programme for an organization should include the following elements:

A. A disaster recovery and business continuity plan, and a definition of access control requirements, human resources and IT fair use policies.
B. Security policy implementation, assignment of roles and responsibilities, and information asset classification.
C. A business impact, threat and vulnerability analysis, delivery of an information security awareness programme, and the physical security of key installations.
D. Senior management organizational structure, message distribution standards, and procedures for the operations of security management systems.

15. As an information systems security manager (ISSM) conducting information security awareness, how would you describe the purpose of your organization's information security policy?

A. A listing of requirements for tools and applications that will be used to protect the system.
B. A definition of key elements (people, process and technology) used in the protection of the organization's systems.
C. A brief, high-level statement indicating what is and is not permitted while handling information in a system.
D. A specification of the defined settings that have been determined to provide optimum security.

Part B – Short Answer Questions – 80 Marks (Overall 80%)

1. Security Policies (12 marks)
   A. Exaplain what you understand by the term 'security policy'. What is the importance of an information security policy?
   B. What is the relationship between a security policy and the corporate objectives of the organization?
   C. some key attributes characterize a good security policy. Identify and describe at least two (2) of such attributes.

2. Concerning the application of policies in information security management, explain the following terms indicating the distinction among them. Using relevant examples, indicate where they apply in an organization. (12 marks)
   A. Programme security policy
   B. Issue-specific policy
   C. System-specific policy

3. **Policy Development Life Cycle:** The diagram below illustrates the typical policy development lifecycle. You have been tasked to develop an **end-user device policy** for your organization. In point form, indicate at least two (2) of the key considerations you would take into account at each stage (Risk Assessment, Policy Construction, Policy Implementation, and Policy Monitoring and Maintenance) of the policy development life cycle. (16 marks)

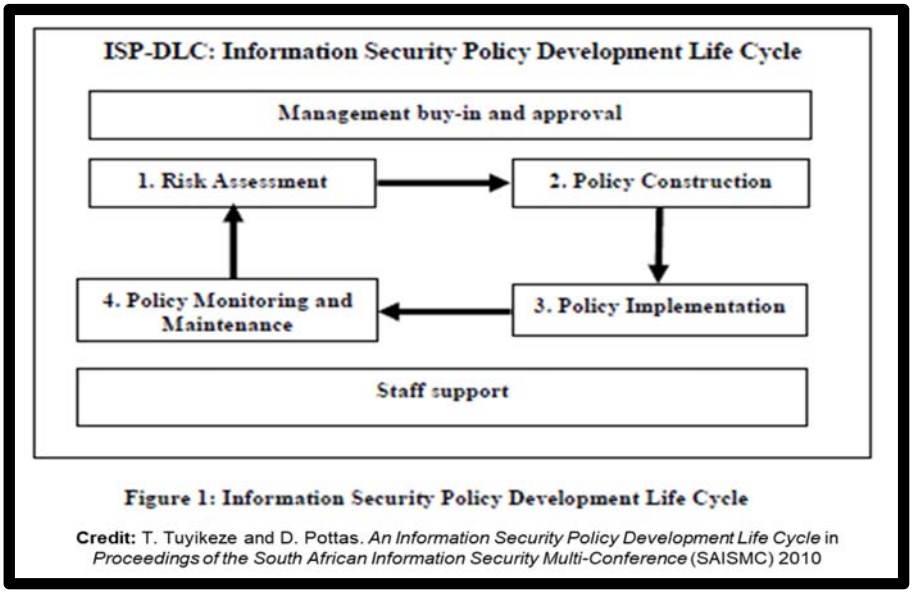

Figure 1: Information Security Policy Development Life Cycle

Credit: T. Tuyikeze and D. Pottas. *An Information Security Policy Development Life Cycle* in *Proceedings of the South African Information Security Multi-Conference* (SAISMC) 2010

4. Information security education, training, awareness and information security policy as a component of policy implementation. (10 marks)

   A. Explain what you understand by security education, training, and awareness programmes. Ensure to distinguish between the three: education, training and awareness.

   B. Explain how a security education, training, and awareness programme supports the implementation of an information security policy in an organization.

5. Information security policy metrics (18 Marks)
   A. Explain what you understand by the term 'information security metrics'.
   B. What is the purpose of these metrics towards achieving the objectives for which the policies were created?
   C. Explain what you understand by behaviour-related metrics. Give at least two examples of such metrics.
   D. Explain what you understand by knowledge-related metrics. Give at least two examples of such metrics.
   E. In your opinion, which one of these two is preferable? Why?

6. Compliance is a key element in information security policy implementation. (8 marks)
   A. Explain what you understand by the term 'compliance'.
   B. Describe at least two (2) major activities organizations undertake as a means of ensuring compliance with a given policy.
   C. What is the role of 'compliance audits' in ensuring policy compliance?

7. Organizations take a special interest in adhering to privacy principles. Concerning this answer the following: (16 marks)
   A. Explain the difference between privacy and security as formally defined.
   B. Expound on the importance of privacy.
   C. Discuss at least 4 key principles that are essential for privacy.
   D. In what ways are the two, i.e. privacy and security, related?

8. A policy must clearly state the roles and responsibilities associated with the successful definition, implementation and maintenance of that policy. (8 marks)
   A. Name at least three (3) roles associated with the effective design, implementation and maintenance of an information security policy.
   B. Why is there a need for clearly articulated roles and responsibilities for any given policy?