Student ID: Number:								
2	3	1	9	9	4	8	0	

Open Questionnaire

Semester 1 2024

Course code:	COMP718
Course description:	Information Security Management
Time allowed:	Upload your answers before 5PM NZ Time.
Date:	Tuesday, 30th July 2024
Total Marks:	40

INSTRUCTIONS

1. The exam comprises 4 main questions. Each main question is worth 10 marks.
2. Ensure that your student ID number is clearly written on each page of the answer sheet.

SUMMARY:

Question	Marks	Suggested time (Minutes)
1.	10	20
2.	10	20
3.	10	20
4.	10	20
Total	**40**	**80**

Note: Please answer all four questions

Question Q1: Data classification is an important part of information security management. Explain why and provide **two** examples.

Question Q2: Quantitative risk analysis estimates the likely losses of future incidents. Explain why achieving accurate results is difficult (provide **two** reasons).

Question Q3: Explain how an organization can prepare for critical system failures through the Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) processes (provide **four** ways).

Question Q4: Provide and describe **two** examples of security controls that are based on the organizational process and employee roles.

ANSWER SHEET

Question Q1:

Data classification is an essential aspect of managing information security, which entails organizing data according to its sensitivity, value, and regulatory needs. This procedure guarantees that data is managed, stored, and transmitted in a way that corresponds to its importance to the organization. Through data classification, organizations can implement security measures that are appropriate to the potential damage that may arise from unauthorized access, disclosure, modification, or deletion.

1. **Personal Identifiable Information (PII):**
   - In the realm of healthcare, it is imperative to categorize patient records that include personally identifiable information (PII) as extremely sensitive. This categorization demands the implementation of sophisticated encryption techniques, stringent access controls such as multi-factor authentication, and routine security assessments to ensure adherence to regulations such as the Health Insurance Portability and Accountability Act (HIPAA).
   - The designation of patient records that contain personally identifiable information (PII) as extremely sensitive is critical in the healthcare industry. To achieve compliance requirements, advanced encryption mechanisms must be used, stringent access restrictions, including multi-factor authentication, must be enforced, and security audits must be conducted on a regular basis in accordance with HIPAA standards.
2. **Financial Data:**
   - In the banking industry, transaction logs and customer account information are considered crucial. This categorization necessitates strong access controls, continuous monitoring for potentially suspicious behavior, and compliance with strict regulatory requirements like PCI DSS in order to thwart financial fraud and data breaches.
   - Within the banking field, transaction logs and customer account particulars are deemed essential. This categorization mandates strong access controls, ongoing monitoring for suspicious activities, and adherence to stringent regulatory standards such as PCI DSS to prevent financial fraud and data breaches.

Question 2:

1. **Imcomplete Data:**
    - Historical records might not encompass all incident categories, particularly those that are infrequent or unprecedented in the organization's setting. This deficiency in inclusive data could result in either underestimating or overestimating risks. For instance, a business may lack adequate data to precisely evaluate the risk of a cyber-attack stemming from a novel malware variant.
    - Past data may not include all event types, particularly those that are unusual or have never occurred in the organization's environment. In the absence of detailed data, dangers can be underestimated or overestimated. For example, a corporation may lack sufficient data to appropriately assess the danger of a cyber-attack originating from a new type of virus.

2. **Uncertainty and Complexity:**
    - The ever-changing characteristics of risks and their interconnectedness contribute significantly to the complexity of risk analysis. Elements like technological progress, shifts in geopolitical landscapes, and the emergence of new threats create uncertainties that conventional statistical models often fail to encompass. An example of this complexity is the challenge of forecasting how a recent regulatory modification will affect business operations, necessitating the consideration of various interacting factors.
    - The complicated linkages between hazards, along with their dynamic character, complicate the risk assessment process. Factors such as technological developments, changes in geopolitical circumstances, and the emergence of new threats add uncertainty that standard statistical methodologies may ignore. For example, assessing the impact of a new regulatory framework on corporate operations necessitates a thorough examination of several factors and their interrelationships.

Question 3:

Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) are fundamentally interconnected, forming a holistic strategy for ensuring organizational resilience. The primary objective of BCP is to sustain essential business operations during disruptions, whereas DRP is specifically concerned with the recovery of information technology systems and data integrity. The alignment of these two plans is crucial, as it facilitates a swift and effective resumption of business activities following a catastrophic event, thereby minimizing downtime and operational impact.

4 ways to prepare:

1. **Risk Assessment:** The process entails the recognition of possible risks such as natural calamities, cyber-attacks, and hardware malfunctions, followed by an evaluation of their probability and potential consequences. By conducting this analysis, organizations can effectively prioritize risks and concentrate on addressing the most crucial areas to ensure business continuity and resilience.
2. **Developing Contingency Plans:** The specified methods must completely explain the specific steps, assigned roles, and resources required for the recovery process following a system breakdown. This includes identifying alternate backup sites, implementing redundant systems, and establishing failover procedures, all with the goal of reducing operational downtime as much as feasible.
3. **Regular Testing:** A range of tests, such as tabletop exercises, simulation drills, and full-scale simulations, are carried out to verify the efficiency of the BCP and DRP. These tests play a crucial role in pinpointing any deficiencies in the plans and guaranteeing that all parties involved comprehend their respective duties and accountabilities.
4. **Continuous Improvement:** It is essential to consistently assess and revise the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) in order to adapt to shifts in the business landscape, advancements in technology, and alterations in organizational structure. This process includes integrating insights gained from previous incidents, revising contact information, and verifying that the plans are still applicable and efficient.

Question 4:

1. **Role-Based Access Control (RBAC):**
   - The control system ensures that workers may only access the data and systems necessary for their responsibilities. For example, a marketing manager could have access to consumer data for campaign analysis but not to the company's financial information. RBAC helps to reduce the risk of insider threats and data abuse by restricting access based on job functions.
   - This control system guarantees that workers only have access to the information and systems required for their jobs. For example, a marketing manager may have access to client data for campaign analysis but not to the company's financials. RBAC helps to reduce the risk of insider threats and data abuse by restricting access based on job functions.
2. **Job Rotation:**
   - The method includes periodically rotating staff to various roles inside the firm. This strategy helps to reduce the chance of fraud and blunders by preventing personnel from becoming too comfortable in one position, where they might exploit flaws. Job rotation also increases employees' talents and comprehension, resulting in a more versatile workforce.
   - Rotating employees to different jobs within the business at regular periods is an important part of this process. This method reduces the danger of fraud and mistakes by preventing personnel from becoming very comfortable in a particular function, where they may exploit weaknesses. Job rotation also improves employees' abilities and knowledge, resulting in a more adaptable workforce.