Student ID: Number:								
2	3	1	9	9	9	3	7	

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 very significant in information security management, because, with its help, organizations secure their private data from unauthorized access, breaches, and losses. Firstly, by classifying sensitive and critical data, organizations can enforce adequate security controls, efficiently distribute resources, and keep up with the regulatory requirements. Below are some essential reasons why we should consider it:

1. More Secure Measure

Data classification inflicts organizations to use security measures which are related to the sensitivity and nature of the data. For instance, data that is highly sensitive may need encryption, access controls, and regular audits, whereas less sensitive data might have fewer restrictions. This means that targeted prevention is completed successfully.

2. Obeying the Law

Lots of industries are managed by laws that require to keep in safety specific data from being damaged. The implementation of data classification guidelines in relation to such laws is useful in avoiding fines, loss of reputation, and as well guaranteeing compliance. A clear classification scheme can ease the way for the auditors to verify their compliance.

Examples of Data Classification

Example 1: Medical Records

In a healthcare setting, patient medical records contain confidential information like medical histories, treatment plans, and personal identification data. This type of data is hewed as shadow Enemy Homes and is protected by regulations that are coercive like HIPAA. Authorized medical personnel can only have access to these records and the data is safeguarded with appropriate encryption and regular audits that are done to prevent unauthorized access and, also, to provide patient confidentiality.

Example 2: Intellectual Property

In the technology company, proprietary software code, patents, and R&D documents are denoted as "Confidential Data". This classification mode helps the organization to enforce strict security measures; for instance, only employee endowed with the highest level of clearance are to be allowed access while other employees have to sign nondisclosure agreements and data should be defended by cyber methods to protect it from unauthorized access and accelerate the organization up against competitors.

Question Q2:

Risk management cannot function without the Quantitative risk analysis which is focused on the possibilities of loss in the future. Nevertheless, to get the precise information could be very difficult because of the multifaceted causes. The following represent the two main reasons for this:

1. Data Limitations

Accurate quantitative risk analysis is based on the scenarios where aversion of loss historical incidents and threats that may occurred has occurred, is present and so on is the model. However, mostly, the necessary data of high quality is not complete, or it does not exist at all. This is especially in the cases of an environment which is quickly changing. Without the supportive data, then when the deflated estimations appear, the risks figure out, which would alternatively exceed the threats and losses are the other way around.

The examples we are going to be using to fit points of a cause of inaccurate risk could be of any material including both overestimation and underestimation of potential risks and losses.

2. Uncertainty and Complexity of Risks

Risks are unpredictable because of many facets such as changing tech, economic conditions, and newly emerged threats a clear-cut case, but all the same are the same. Every so often, numerous risks from different sectors have been affected due to the unpredictability of these circumstances. Also, all areas like the migration of risks due to interdependency which becomes difficult in the analysis of risks. Hence, the accuracy and preciseness in risk modelling demand an expert in the specific area and instead of good results, it can sometimes generate unexpected errors in risk estimation.

Question Q3:

1. Risk Assessment and Business Impact Analysis

The sort of the identified critical system can be as a result of this, the study conducted should include system criticality, identification of crucial assets, and the potential effects of unavailability on the organization. The focus of the above analysis should be on the threats, the vulnerabilities, and the way the critical system failures might lead to disaster. This information for decision-makers can be really helpful in arranging the activities. Positive management will quickly decide first how to with the new capacity. Then, they can go back and learn the dispossession of servers which require downtime to move the data. Findings: documentaries, working sessions, and risk management tables. A document has been reviewed with suggestions and fixed.

2. Developing and Testing Recovery Strategies

After recognizing the critical systems in a business, organizations should draft precise recovery strategies as part of their efforts aimed at returning to their normal operations as soon as possible after a disaster. Different software and hardware devices like backup systems, Data recovery processes, and alternative communication channels can also be used for this. Mapping is done to define the maps it wants to use with respect to the backups. <p> does not count as content. It will be the same as my content but uploaded using the proper HTML tags. FMAS – FDT complexity is here as large trees are involved. Department(s) shall assign or certify a provider to fill in the gaps if there are any. Employees received training about roles and procedures in case of a system failure.

3. Maintaining Updated Documentation

Contact lists, recovery procedures, and resource listings should be covered in the documentation and often checked to ensure everything is still accurate. Both training management and training resources have come out with methods that can be run one-to-one. The information on risk analysis and management may come out of different systems or department Delegations of responsibilities between staff members and quality control personnel will be better just surveillance rather than good personnel are provoked. Upon gaining a leadership role, some managers choose to keep their options open by treating their subordinates poorly.

4. Employee Training and Awareness

Participants of all training should undergo a short study to know the continuity of Business planning from Business recovery. People who are adverse to updating are not only irrational (as they waste a very precious resource: time) but will also have some serious technology problems. Some nations like Australia, Hungary, Ireland, & Canada agreed that more tests were warranted. Back to the point of technology use and surveillance issues friends can evaluate the evidence together and then come to a consensus about the fact that, overall, technology use and violations of privacy are more important than if technology is the cause for the violation. Offered training is valid for one year after the date recorded in the registration system of the trainer. A record will be kept of the modules that each employee has had, even if the system does not. The device is powered by a personal SIM card connected to the network via Bluetooth. Currently, the SIM card is embedded in the technology to communicate with local and foreign servers. In fact, it uses hardware and software to do things when it is operating.

Question Q4:

Security controls are the mainstay of an organization in protecting assets and information. Their harmonious incorporation into various organizational and employee functions also contribute to the improvement of security sense. Following are a couple of illustrations:

1. Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) is a security model that allows the system to be accessed only by the authorized users aligned with their duties in the company. In this model, the role is associated with the given permissions, instead of users, which eases out the administration works and provides better security.

Description: For example, An organization may adopt a new security strategy by categorizing their employees into roles like "Administrator," "Manager," and "Employee." The roles are the things that define what data and systems every enrolled can access. The Administrators can exert the controlling power over the entire system by being able to effectively manage the settings and configurations, however, staff may only access the data that is assigned to them and the relevant department files.

Benefits: This control measure allows secure access that employees use only to reach the necessities of their work, thus it lowers the amount of accidental or intentional data thefts. Regular checks and role reviews would manage to maintain the access to levels required.

2. Security Awareness Training

Security Awareness Training is an educational course that focuses on security issues, policies, and best practices in an organization. This training program is usually fixed to job roles, thereby ensuring that the staff fully are aware of the importance of information security. Security Awareness Training is a must-have that gears up employees with the knowledge and skills to minimize cybersecurity- related risks.

Phishing Simulation Training is developed for teaching the employees about the dangers of phishing attacks and how to react to them correctly, said the organizers. The training is often accompanied with real-time simulations of phishing attempts.

Description: For example, a company might hold regular phishing simulation sessions where employees receive simulated phishing emails that replicate real-world attacks. Treachery tools like links or attachments are sent in these mails that may enable systems of the company to malfunction or would just send the users to bogus sites. After the completion of the exercise, the employees who interacted with the pretend phishing would not only receive feedback about their actions but would be given instruction to recognize phishing emails in the future.

Benefits: The employees by taking part in phishing simulations become more educated and aware of the counterfeit means of phishing to follow. They are then able to reduce the likelihood of phishing attacks by taking a proactive stand which in turn safeguards personal Information and lessens the impact of data breaches. In addition to averting cyber-attacks, regular simulations will also contribute to the organization's cybersecurity policy, hence, all staff members will participate and develop an understanding of security.