CRT02

UNIVERSITY OF BOLTON

SCHOOL OF CREATIVE TECHNOLOGIES

BSC (HONS) COMPUTING (CYBER SECURITY)

SEMESTER 1 EXAMINATION 2023/24

INFORMATION SECURITY MANAGEMENT

MODULE NO: SEC6203

Date: Friday 12th January 2024 **Time: 10:00 – 12:00**

INSTRUCTIONS TO CANDIDATES:

There are FIVE questions on this exam brief.

Answer ANY FOUR of the five questions

All questions carry equal marks.

School of Creative Technologies
BSc (Hons) Computing (Cyber Security)
Semester One Examination 2023/24
Information Security Management
Module No: SEC6203

Question 1

(i) Examine the foundational principles that serve as the building blocks for the development of security systems. **(10 Marks)**

(ii) Provide examples of at least five of these principles and how they can be applied to enhance an organization's overall cybersecurity posture. **(10 Marks)**

(iii) Additionally, discuss the potential challenges organizations might face when attempting to implement these principles effectively. **(5 Marks)**

Total 25 marks

Question 2

(i) Analyse the significance of adopting national and international standards and frameworks in information security management. **(10 Marks)**

(ii) Provide examples of specific standards or frameworks and explain how they can help organizations address cybersecurity challenges and regulatory compliance.

(10 Marks)

(iii) Additionally, highlight the potential benefits associated with implementing these standards within Jupiter Insurance **case study (see page 5 and 6)**. **(5 Marks)**

Total 25 marks

PLEASE TURN THE PAGE

School of Creative Technologies
BSc (Hons) Computing (Cyber Security)
Semester One Examination 2023/24
Information Security Management
Module No: SEC6203

Question 3

More than ever organizations have legal responsibility to ensure that their organizational data and that of their customers are secure, private, and safe from breaches or damage. Therefore, organizations must ensure a periodic and thorough security audit to be carried out to assess and mitigate various risks to information and information systems using various standards and frameworks.

(i) Conduct a comprehensive analysis of one of the prominent risk management standards, such as NIST (National Institute of Standards and Technology) or ISO (International Organization for Standardization), emphasizing its key principles and methodologies. **(10 Marks)**

(ii) Additionally, critically assess the paramount importance of information risk management and compliance within the context of the attached **case study (see page 5 and 6)**. **(15 Marks)**

(Total 25 Marks)

Question 4

There is a key role of Cryptography in securing and protecting information in transit and at rest.

(i) Evaluate the effectiveness of encryption and hashing methods in upholding the principles of confidentiality, integrity, and availability. **(10 Marks)**

(ii) Additionally, conduct an analysis of how asymmetric encryption, specifically through Public Key Infrastructure (PKI), safeguards information against unauthorized access and disclosure. **(15 Marks)**

(Total 25 Marks)

PLEASE TURN THE PAGE

School of Creative Technologies
BSc (Hons) Computing (Cyber Security)
Semester One Examination 2023/24
Information Security Management
Module No: SEC6203

Question 5

(i) Examine the Case Study provided (refer to pages 4 and 5) to identify a range of threats and vulnerabilities that pose risks to the organization's data, systems, and networks. **(10 Marks)**

(ii) Following this analysis, propose a comprehensive security control solution designed to mitigate these identified risks. This solution should incorporate a defense-in-depth strategy, integrating various access control mechanisms to fortify the organization's security posture. **(15 Marks)**

(Total 25 Marks)

END OF QUESTIONS

PLEASE TURN THE PAGE FOR CASE STUDY…

School of Creative Technologies
BSc (Hons) Computing (Cyber Security)
Semester One Examination 2023/24
Information Security Management
Module No: SEC6203

Case Study

Jupiter Insurance has more than quarter of a million customers and offers a range of insurance services to their customer. The company specializes in providing outstanding service, customer satisfaction, secure information management and protection of sensitive data.

The company has an impressive IT infrastructure and most if not all its operations are highly integrated and dependent on its IT assets. These IT assets include the data and information of customers, employees, vendors and partners and the information processing systems which store, process and transmit them. Therefore, these IT assets are the life blood of the company and must be protected against all threats.

The company is subject to a wide range of legislative, regulatory and contractual obligations that necessitate the protection and security of its IT assets. The objective of the Corporate Information Security and Risk Management policy is to declare the management's dedication and endorsement of safeguarding these assets. It also aims to define the framework and environment employed by the company to ensure the protection of IT assets against all forms of threats, whether originating internally or externally, intentional, or unintentional.

Several issues have been identified in the areas of logical security and change management. Regarding logical security, deficiencies have been observed, such as the sharing of administrator accounts and the lack of sufficient controls over passwords. These vulnerabilities pose a risk to the confidentiality and integrity of the organization's sensitive data. In terms of change management, deficiencies have been found in the segregation of incompatible duties and the inadequate documentation of changes. Furthermore, the process for deploying operating system updates to servers was found to be only partially effective.

Inconsistencies were found in the encryption policy (issues around digital certification management) and data classification policy that involves encoding data to prevent unauthorized access and help protect data in transit and at rest.

CASE STUDY CONTINUED OVER THE PAGE

School of Creative Technologies
BSc (Hons) Computing (Cyber Security)
Semester One Examination 2023/24
Information Security Management
Module No: SEC6203

CASE STUDY CONTINUED

There are unresolved incidents and have been pending escalation indicating a potential lack of proper incident handling procedures or a breakdown in the incident response workflow. The nature of incidents reported were related to data loss due to backup error, malfunction of the web application and intermittent internet connection due to faulty and misconfigured networking devices and firewall. There are no clear criteria and parameters set for assigning the priority of these incidents.

The organization has recently embraced a hybrid cloud platform by adopting IaaS model and is currently undergoing application migration. However, the migration process has encountered challenges, resulting in potential risks associated with data exfiltration during the cloud adoption journey. There are risks particularly relating to network segmentation, IAM and data classification.

The company needs a broad package of support to help it meet a wide range of cyber security, privacy and regulatory requirements, especially the one under GDPR and PCI DSS to improve its overall IT security governance. Business must consider how information is exchanged and stored as it is subject to these regulations which influence its information security policy and practices

END OF PAPER