[CRT02]

UNIVERSITY OF BOLTON

SCHOOL OF CREATIVE TECHNOLOGIES

BSC (HONS) COMPUTING (CYBER SECURITY)

SEMESTER ONE EXAMINATION 2022/23

INFORMATION SECURITY MANAGEMENT

MODULE NO: SEC6203

Date: Monday 9th January 2023 **Time: 14:00 – 16:00**

INSTRUCTIONS TO CANDIDATES: There are **FIVE** questions on this exam brief.

Answer **ANY FOUR** questions

All questions carry equal marks.

The case study is provided on pages 3 and 4

School of Creative Technologies
BSc (Hons) Computing (Cyber Security)
Semester One Examination 2022/23
Information Security Management
Module No. SEC6203

1. Analyze the importance of an Information Security policy as a strategy to achieve long term objectives of the organization within the **Case Study**. Assess various principles that govern those goal and objectives. Evaluate various characteristics of a policy as a document and ways it could be implemented.

(25 Marks)

2. A much higher level of security is required when translating confidential information. Data is an important asset and has various forms, some need protection and others don't. Analyze various data classification techniques and their importance and how these techniques can be implemented as strategy for the security management of an organization firstly, to help ensure compliance with PCI DSS and secondly, to use as a guideline for mapping types of information security to categories of security controls.

(25 Marks)

3. The digital age in which we live has necessitated that data and information are kept safe. More than ever organizations have legal responsibility to ensure that their organizational data and that of their customers is secure, private, and safe from breaches or damage. **Having familiarized yourself with the attached Case Study**, **critically analyze the importance of Information risk management and compliance** and contrast the relevant standards and regulations regarding compliance.

(25 Marks)

4. Evaluate the information security posture of the organization in the **attached Case Study** and identify various threats and vulnerabilities to data, systems and networks. Devise a security control solution to mitigate those risks using defense-in-depth mechanism and access control solutions to mitigate those risks.

(25 Marks)

PLEASE TURN THE PAGE….

School of Creative Technologies
BSc (Hons) Computing (Cyber Security)
Semester One Examination 2022/23
Information Security Management
Module No. SEC6203

5. Cryptography plays an important role in securing and protecting information in transit and at rest. Assess the effectiveness of encryption and hashing techniques and their role in providing confidentiality, integrity and availability. Analyze the role of asymmetric encryption (Public Key Infrastructure) in protecting information from unauthorized access and disclosure.

(25 Marks)

END OF QUESTIONS

Case Study

You have been hired as CISO by insurance company to develop information security program to protect data and information system from cyber breaches. This will allow the senior management to ensure the proper creation, implementation and enforcement of a security policy.

The company has more than quarter of a million customers and offers a range of insurance services to their customer. The company's objective is to provide 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 as well as the information processing systems which store, process and transmit these assets. 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 agreements and specifications, which also requires the proper protection and security of all these IT assets. The purpose of this Corporate Information Security and Risk Management is to state the commitment and support of management to such protection and security, and to specify the environment which will be used in this company to protect these IT assets from all types of threats, whether internal or external, deliberate or accidental.

Case study continues over the page….

School of Creative Technologies
BSc (Hons) Computing (Cyber Security)
Semester One Examination 2022/23
Information Security Management
Module No. SEC6203

Case study continued….

Problems have been identified in the areas of logical security and change management. Logical security deficiencies noted included the sharing of administrator accounts and failure to enforce adequate controls over passwords. Change management deficiencies included improper segregation of incompatible duties and failure to document all changes. Additionally, 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.

There are unresolved incidents and have been pending escalation. The nature of incidents reported were related to data loss due to backup error, malfunction of the web application and intermittent internet connection possibly due to faulty and misconfigured networking devices and firewall. There is no clear criteria and parameter set for assigning the priority of these incidents.

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. The business must consider the how information is exchanged and stored as it is subject to these regulations which influence its information security policy and practices.

END OF PAPER