JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF SCIENCE IN IT SECURITY AND AUDIT

YEAR 1 SEMESTER 2

2023/2024 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT5211

Course Title: Security Policies, Standards and Compliance Strategies

EXAM VENUE: **STREAM:**

DATE: **EXAM SESSION:**

TIME:

INSTRUCTIONS

---

1. Answer any **THREE** questions.
2. Candidates are advised not to write on the QUESTION paper
3. Candidates must hand in their answer booklets to the invigilator while in the examination room
4. No Mobile devices are allowed into the Examination Room

QUESTION ONE **(20 MARKS)**

(a) A major UK bank has decided to overhaul its aging systems, which manage all branch activities. The following aims have been identified as particularly important: the systems must prevent unauthorized access, both to prevent fraud, and also to preserve customer confidentiality; the system must be able to cope with peak processing loads without undue delay; the full range of business processes must be supported, with emphasis for allowing easy amendment to functionality in the future; through-the-wall banking (ATMs) and home-banking must be available 24 hours a day, 365 days a year; calculations carried out by systems must be fool-proof, so as to avoid dissatisfied customers and bad PR; computers at the corporate data center must be able to easily communicate with branch machines and terminals, and also with other banks in the UK and abroad.

Using an appropriate risk model, discuss the risk issues that should be addressed. (8 Marks)

(b) Discuss best practices for managing Vendor security risk (12 Marks)

QUESTION TWO **(20 MARKS)**

(a) Discuss the need for banks world-wide to embrace the Gramm-Leach-Bliley Act (GLBA) (5 marks)

(b) Discuss the need for a government embracing the Sarbanes-Oxley (SOX) Act. (5 marks)

(c) Discuss security techniques to formulate, administer, audit, manage and evaluate network security policies and standards based on best practices and standards (10 Marks)

QUESTION THREE **(20 MARKS)**

Discuss the following standards in relation to data protection control and compliance.

(a) ISO 17799/27001 standard (6 marks)

(b) Payment Card Industry (PCI) Data Security Standard (7 marks)

(c) KEBS security policies and standards. (7 marks)

QUESTION FOUR **(20 MARKS)**

Read the Case study below and answer the questions that follow.

Case study: Stolen Hospital laptop causes heartburn

SCENARIO:

A healthcare system executive left their work-issued laptop, which had access to over 40,000 medical records, in a locked car while running an errand. The car was broken into, and the laptop stolen.

ATTACK:

Physical theft of an unencrypted device.

RESPONSE:

The employee immediately reported the theft to the police and to the healthcare system's IT department who disabled the laptop's remote access and began monitoring activity. The laptop was equipped with security tools and password protection. Data stored on the hard drive was not encrypted – this included sensitive, personal patient data. The hospital had to follow state laws as they pertain to a data breach. The U.S. Department of Health and Human Services was also notified. Personally Identifiable Information (PII) and Protected Health Information (PHI) data require rigorous reporting processes and standards.

After the theft and breach, the health care system began an extensive review of internal policies; they created a discipline procedure for employees who violate security standards. A thorough review of security measures with internal IT staff and ancillary IT vendors revealed vulnerabilities.

IMPACT:

The healthcare system spent over Ksh.2,000,000 in remediation, monitoring, and operational improvements. A data breach does impact a brand negatively and trust has to be rebuilt.

Required:

(a) (i) Explain the term encryption as used in this scenario (2 Marks)

(ii) Highlight **THREE** steps that the company could have taken to prevent this incident (3 Marks)

(b) Discuss the importance of Business continuity planning to an organization (5 Marks)

(c) Discuss any **FIVE** lessons learned from the attack (10 Marks)

QUESTION FIVE **(20 MARKS)**

(a) Describe what constitutes a breach under Health Insurance Portability and Accountability Act (HIPPA) rules (2 marks)

(b) Explain how the HIPPA security rule differs from the Privacy rule (4 marks)

(c) Discuss the roadblocks to web usage beyond the availability of the technology (6 Marks)

(d) Compare and contrast the COBIT and NIST frameworks in relation to risk management (8 Marks)

This is the last printed page