SPECIFY TYPE OF EXAMINATION	
FIRST ATTEMPT	☐
FIRST RESIT	☐
SECOND RESIT	☐
RE-TAKE	☐

JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS & INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF MASTERS OF INFORMATION TECHNOLOGY SECURITY AND AUDIT

2TH YEAR 1ST SEMESTER 2022/2023 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT 5212

COURSE TITLE: ADVANCED INFORMATION SYSTEMS CONTROL AND AUDIT

DATE: **TIME:**

TIME: 2 HOURS

Instructions:

1. **This paper contains FIVE questions**
2. **Answer any THREE questions**

Question 1 - <u>Shining Tor Ltd - Basic Security Audit Case Study</u> (20 marks)

Shining Tor Ltd were unfortunate enough to have suffered a major data breach in August 2018 where 500,000 of their customers' accounts were compromised in a hacking attack. Romano Security Consulting were invited to conduct a Basic Security Audit at Shining Tor's London offices in September 2018, with the purpose of assisting the Senior Management team in developing a strategy for managing their cyber and information security.

Romano Security Consulting held an initial scoping call with Shining Tor's CEO to establish their requirements and to gather some further details around the August hacking attack. Following the scoping call it was decided that given the relatively low level of security maturity within the organization that Romano Security Consulting's recently developed Basic Security Audit service offering would be the best fit for the organization. This was agreed with the CEO and a statement of work was signed off.

The Basic Security Audit has been devised to specifically focus on evaluating an organizations cyber security risks in 3 main areas people, processes, and technology and provide high level recommendations on how identified risks can be speedily mitigated. This entry-level security audit is particularly valuable to organizations who have yet to evaluate and document their risks, vulnerabilities and threat exposure.

The Basic Security Audit is based around the CIS 20 Critical Controls, 10 steps to Cyber Security, ISO 27001:2013, Cyber Essentials and industry best practice. The security audit began with a detailed overview of the organization, its IT infrastructure and a detailed account of the hacking attack that occurred in August 2018. The CEO and several of the functional managers including the Development, IT and Operations Managers were interviewed during the security audit. The following Non-Technical and Technical control areas were covered during the audit:

- Cyber and information security Governance, Data Security, Cyber Risk Management, Training and Awareness, Legal, Regulatory and Contractual Requirements, Policies & ISMS, Business Continuity and Incident Management, Physical Security, Third party Supplier Management, Secure Development
- Hosting, Secure Configuration, Network architecture, Secure Perimeter – Firewalls, IDS, data exfiltration, Anti-Malware, Access Control, User Privileges, Mobile devices, mobile working and removable media, Security Monitoring

Findings and recommendations were made during the security audit as and when they were identified. A sample of the recommendations made following the security audit are below:

- Assign accountability and responsibility for security to an individual or individuals
- Compile a high level risk register, develop a suitable risk management framework, conduct a risk assessment at regular intervals the organizations assets and apply controls applied where applicable
- Provide security awareness training to all staff on induction and communicate security updates at regular intervals

- Implement a door pass card system, Implement a clear desk and clear screen policy, Secure unattended offices, server rooms and filing cabinets
- Document and communicate an incident management process, Document incident response plans for different scenarios
- Carry out third party risk supplier risk assessments
- Implementation of the required controls to comply with the GDPR regulations
- Establish ownership and administrative control of the external firewall, Purchase and deploy a suitable internal firewall (hardware or software)
- Document and implement a patching policy for all hardware and applications, Check AV is currently up to date on all devices
- Introduce RBAC (role based access) for Dropbox (internal and external), Document and review user access for all applications,
- Encrypt all mobile devices and removable media
- Avoid storing un-encrypted customer data (locally). Encrypt all data in storage and transit

The following high level recommendations were made:

- Implementation of ISO 27001:2013 and Cyber Essentials and regular penetration testing

A summary report was provided to Shining Tor's CEO following the Security Audit and a follow up call was arranged with Romano Security Consulting to walk through the findings and recommendations. Romano Security Consulting are currently assisting Shining Tor in their audit remediation and the implementation of ISO 27001. Regular penetration testing is now being carried out on Shining Tor's IT infrastructure.

a) Discuss clearly any FIVE sources of evidence that you would anticipate that Romano Security Consulting could have focused on during the process of audit evidence collection. (10 marks)
b) During the process of conducting the audit, Romano Security Consulting should have been familiarized with some of the risk factors that may be inherent in business operations as they review the risk analysis done by Shining Tor. Discuss any FIVE of these risk factors. (10 marks)

Question 2 (20 marks)

a) Discuss the three major aspects that an IS auditor should consider when undertaking the design of a questionnaire to be used during the audit procedure. (6 marks)
b) Discuss the five main phases that an auditor assesses in the process of hardware acquisition. (10 marks)

Question 3 - AlphaCo Hacking incident: Case Study (20 marks)

In early 2002, the accounts receivable department of AlphaCo discovered a significant amount of uncollected accounts while performing an aging analysis. These accounts totaled in the millions and were tracked to shipments to an Aegean Island. Several of the accounts were listed under the same address. Further reviews revealed that the accounts were fraudulent. A hacker penetrated the online order management system of the firm, created fake accounts and placed about 50 fraudulent orders over a period of three months and stole shipments that have a value of approximately $20 million.

When they called the phone number listed in the fraudulent accounts, to their surprise, AlphaCo representatives were able to reach the hacker, who seemed to be waiting for the AlphaCo's call. The hacker threatened that unless the firm paid him $10 million, he would publish IT security vulnerabilities of the firm and his hacking techniques on the Internet and harm AlphaCo's reputation. AlphaCo immediately contacted law enforcement agencies. In recent years, these kinds of hacking incidents and extortions were on the rise. Thus, the law enforcement agencies viewed this as a serious crime and a major threat to electronic commerce and the integrity of data that the financial community relies upon to do business nationally and internationally.

With the knowledge of the law enforcement agencies, AlphaCo entered negotiations with the hacker. While the effort to catch the hacker was underway, AlphaCo brought in computer forensics experts and IT security consultants to investigate how exactly the online order management system had been breached.

Assume you work for the IT security consultant firm that has been hired by AlphaCo.

a) To understand the challenge with AlphaCo's online order system, you have to conduct an extensive audit on the e-commerce environment that they have in place. Discuss any FIVE objectives that you want to achieve in conducting this audit. (10 marks)
b) Discuss any FIVE aspects that you would consider during the review of the Internet Security Administration functions of the e-commerce system put in place by AlphaCo. (10 marks)

Question 4 (20 marks)

a) Explain FOUR areas where an IS auditor is needed so as to assist a financial auditor during an audit. **(8 marks)**

a) Discuss clearly the three different procedures that can be used when doing sampling during an audit and give examples for each procedure. **(6 marks)**
b) Discuss the three major aspects that an IS auditor should consider when undertaking the design of a questionnaire to be used during the audit procedure. **(6 marks)**

Question 5 - Bleaklow Ltd - ISO 27001 Audit Case Study (20 marks)

Bleaklow Ltd is a mature Information Management & Technology provider for services and technological solutions to over 100 NHS organizations throughout the UK. Bleaklow Ltd utilize a Microsoft Exchange email system which they have developed to a secure specification and wanted to provide this email service to their clients as an alternative to the secure NHS 2 mail system that the NHS provides. In order to be able to utilize and provide this email service for communicating confidential data Bleaklow are required to comply with the NHS ISB 1596 Secure Email Specification.

The NHS ISB 1596 Secure Email Specification defines the minimum non-functional requirements for a secure email service for the storage and transmission of patient identifiable data by an email system. The requirements of NHS ISB 1596 state that health and care organizations must operate their email service to at least the level of security standard ISO/IEC 27001:2013 and that this must be audited.

The organization that manage the NHS security HSCIC (Health and Social Care Information Centre) required Bleaklow to engage a suitably qualified company to provide audit assurance that Bleaklow had a suitable information security management system and the necessary security controls in place. Romano Security Consulting were verified by HSCIC as having the skills, experience and qualifications to provide this level of assurance. Bleaklow have developed an ISMS to manage the security aspects of the Microsoft Exchange email system and Romano Security Consultancy was identified as a company that has the experience to provide an independent ISO 27001 internal audit of the ISMS.

During an initial scoping discussion held in August 2018 Romano Security Consulting provided information about the relevant services that we could supply and subsequently drafted a detailed statement of work which took into consideration the requirements discussed during the scoping discussions. The statement of work clearly detailed all the resources and costs necessary to meet the client's stated objective so that they would be able to achieve this without the need to allocate any additional budget and would also be within the tight timeframes specified by Bleaklow. The scope of the audit was agreed with Bleaklow and covered the Microsoft Exchange email system and assessed the service against the requirements of the following areas from ISO 27001:2013:

- ISO 27001 ISMS Framework Sections:
    - 4.3 Scope
    - 5.2 Policy
    - 6.1, 8.2, 8.3 Risk Assessment and Risk Management
    - 7.3 Awareness
    - 9.2 Internal Audit
- ISO 27001:2013 Annex A Sections
    - A8 Asset Management
    - A9 Access Control
    - A10 Cryptography
    - A11 Physical and Environmental
    - A12 Operations Security

- A13 Communications
- A16 Incident Management
- A17 Business Continuity Management

The ISO 27001 audit consisted of face-to-face interviews with key member's staff such as the Head of Governance and Assurance, IT and Infrastructure Manager and Network Manager and an examination of processes and process documentation. The audit was completed against the requirements of ISO 27001:2013 and the data reviewed was used to provide an informed ISO 27001 compliance assessment.

Following the audit, a detailed audit report was provided to Bleaklow. The report consisted of a detailed summary of the audit, findings and recommendations for corrective actions. There were a number non-conformances and observations recorded as a result of the audit. A corrective action plan was drawn up with Bleaklow and Romano Security Consulting and as part of the audit brief Romano Security Consulting were also asked to provide advice on the corrective actions for the non-conformances and observations. The remediation advice largely consisted of recommendations of changes to documentation, processes and controls. Bleaklow implemented the suggested corrective action recommendations and provided the necessary evidence to close off the non-conformances and observations.

Once all of the findings had been closed off, Romano Security Consulting were asked to provide a statement to HSCIC to confirm that Bleaklow infrastructure, processes and controls supporting the secure email system complied with the requirements of ISO 27001:2013 and the NHS ISB 1596 specification. In October 2018 Bleaklow were awarded the accreditation from HSCIC that they required for their secure email system. Bleaklow are now able to provide their secure email system to their clients and partners. Romano Security Consulting have agreed a contract with Bleaklow to audit their secure email system on an annual basis.

a) Clearly discuss the five business continuity planning strategies that Romano Security Consulting should be looking for when they audit Bleaklow. **(10 marks)**
b) The Romano Security Consulting needs to be satisfied that the Bleaklow uses documents necessary for a smooth roll out of the business resumption plan. Discuss any five forms or documents that they should be looking for. **(10 marks)**