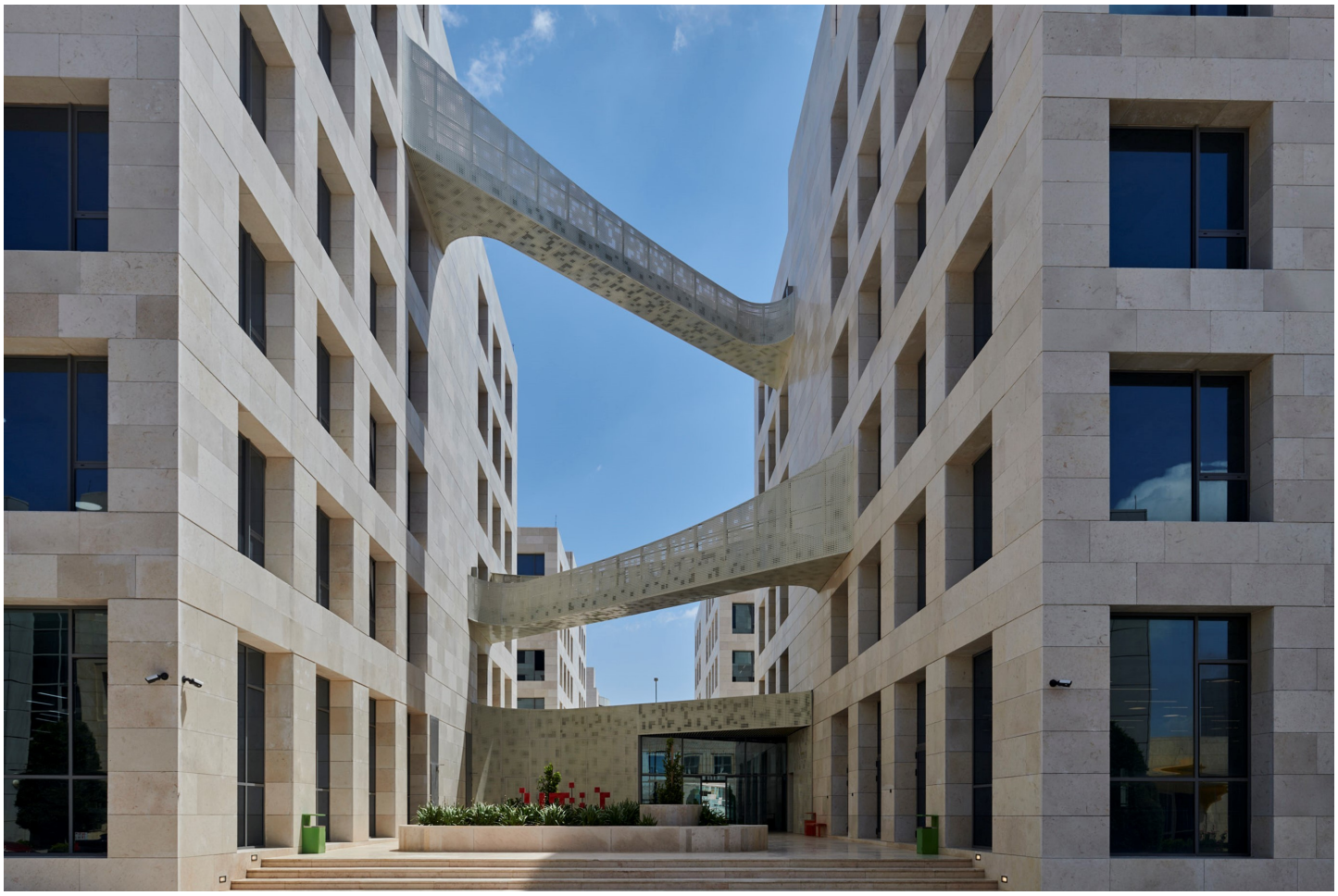
جامعة الحسين التقنية
Al Hussein Technical University

ASSIGNMENT BRIEF

HTU Course No: 10203300	**HTU Course Name:** Information Security Management
BTEC Unit Code:	**BTEC UNIT Name:**

Version: 1



Student Name/ID Number/Section	
HTU Course Number and Title	10203300 Information Security Management
BTEC Unit Code and Title	
Academic Year	2023-2024 Spring
Assignment Author	Eman Alzyoud
Course Tutor	Eman Alzyoud
Assignment Title	ISMS Assignment
Assignment Ref No	1
Issue Date	16/04/2024
Formative Assessment dates	From 17/04/2024 to 30/05/2024
Submission Date	12/06/2024
IV Name & Date	Salem Alemaishat 15/04/2024

Submission Format

Each student is expected to individually submit his/her work , including:

1. Cobit 19 foundation certificate from ISACA.
2. Cobit 19 design and implementation certificate from ISACA.
3. Student declaration form.

OR

1. An individual written report in Word covering the required details in the Assignment Brief and Guidance section. Including a signed student assessment submission and declaration form.
2. Evidence of the implemented framework (a soft copy of the ISACA toolkit). Students should use the ISACA toolkit.

Files should be uploaded separately rather than in a zip file.

Report guidelines:
The report should be written in a concise, formal business style using single spacing and font size 12 with the use of headings, paragraphs, and subsections as appropriate (a cover page, table of contents, and an introduction to provide an overview of your report.). The expected word limit is about 5000 words, although you will not be penalized for exceeding the total word limit. The report must be supported with research and referenced using the Harvard referencing system. The eligible Turnitin percentage is 15%.

Notes:

- If you do not see the Turnitin report when you initially submit your report, contact your instructor immediately.

- Oral Exam: An oral Discussion about the report and the implemented work. Instructions, dates, and times for the discussion will be provided later. A student's final grade will depend on both the technical report AND the oral assessment.
- Resubmission: If you lose two or more Ps, you will NOT be eligible for resubmission.
- Soft copy submissions should be done through the university's eLearning system https://elearning.htu.edu.jo by the deadline assigned above.

Unit Learning Outcomes

LO1 Explore the basic principles of information security management.

LO2 Critically assess how an organization can implement and maintain an Information Security Management System (ISMS).

LO3 Appraise an ISMS and describe any weaknesses it may contain.

LO4 Examine the strengths and weaknesses of implementing ISMS standards.

Assignment Brief and Guidance

Option 1:

If the university provides exam vouchers, students can register for the two exams on the ISACA website before 12 June. Choose exam dates with a one-month gap between the two exams. After passing both exams, submit the Cobit 19 foundation certificate in addition to Cobit 19 design and implementation certificate on the e-learning system.

https://www.isaca.org/credentialing/cobit-foundation#register

the exams are:

Cobit 19 foundation.

Cobit 19 design and implementation.

The Cobit 19 foundation certificate covers P1, P2, M1, M2, and D1 criteria, while Cobit 19 design and implementation certificate covers P3, P4, P5, M3, M4, and D2 criteria.

If the student did not register for the exams, he/she can proceed with option 2 of the assignment brief.

Option 2:

Case Study Synopsis:

We will be using Bluefrontier Bank as an exemplar model in this Information Security Management System (ISMS) project assignment. Bluefrontier Bank is a well-established bank that offers a comprehensive end-to-end service, including Loans, Business Banking such as Business loans), checking accounts, Savings accounts, Debit and credit cards, Merchant services (credit card processing, reconciliation, and reporting, and Treasury services. In addition to Digital Banking including Online and mobile banking, Text alerts, e-statements, and Online bill pay.

Bluefrontier Bank gained multiple certifications from ISO, and the Managing Director (MD) has decided and set a strategic plan for the bank to design and implement the Cobit 2019 standard.

The bank recognized that such a decision is vital to meet the business needs/operations amid various laws and regulations.

Using the ISACA toolkit , you must conduct a design factor study based on the following factors:

1. The strategy of the bank

Banks' strategy includes embracing digital transformation and fintech and partnering with fintech for innovative technologies. Building trust with customers, improving customer experience, and outsourcing non-differentiating activities to modular utilities can increase productivity. Adopting digital and non-digital capabilities can give a company a competitive edge. Fostering a strong employee culture and prioritizing remote worker considerations are also essential.

2. Company goals that support the company strategy.

- Maximize profits
- Launch new products
- Improve customer service
- Increase management efficiency
- Become a thought leader or industry expert
- Rank higher on the search engine results page
- Increase the company’s social media presence
- Create an employee reward or loyalty program

3. The IT risk profile of the company to which the company is exposed.

A screenshot from the IT risk profile is shown below.

Deficiency in the ATM Machines Monitoring Coverage	Reputation/Good will	2	Medium	Low
ATM Security breaches	Cash/profitability	2	Medium	Low
Misleading Analysis of ATM Switch Failure	Reputation/Good will	3	Medium	High
ATM software/hardware failure	Reputation/Good will	3	Low	Low
ATM traffic is hacked and decrypted	Reputation/Good will	2	High	Low
Mobile Banking "Interception of traffic"	Cash/profitability	2	Medium	Low
Compromised Mobile Banking Security	Reputation/Good will	2	Medium	Low
Mobile banking Poor Password Protection	Reputation/Good will	2	Medium	Low
IBS hack CUSTOMERS password BY Keyloggers	Reputation/Good will	2	Medium	Low
ECC server fails	Cash & Legal	4	High	Low
Integration between ECC and CORE banking	Cash & Legal	3	Medium	Low
E-banking server is down for a significant period	Reputation/Good will	3	Medium	Low
E-banking comms link down for a significant time	Reputation/Good will	3	High	Low
Denial of service attack	Reputation/Good will	2	High	High
Patches/upgrades degrade e-banking system	Reputation/Good will	3	Medium	Medium
SWIFT system/link down for a significant period	Reputation/Good will	3	High	Low
Insecure Protection of LSO/RSO Passwords for Emerg	Cash/profitability	2	High	Low
Safewatch " Delay in uploading Blacklists "	Cash & Legal	3	High	Low
Non-Updated Version of en.Safewatch Filtering Syst	Cash & Legal	2	High	Low
SMS/mobile server is down for a period	Reputation/Good will	3	Medium	Low
Failure of SMS alerts for customers transactions	Reputation/Good will	3	Medium	Medium
Help Desk issues/incidents not resolved promptly	Cash/profitability	4	Medium	Medium
End of Day procedure not run	Reputation/Good will	4	High	Low

4. I&T risks or matters that have already materialized.

- Communication barriers arise between information & technology specialists and business users due to the gap between their technical and business understanding. recurring problems with the integration of data across and the quality of the data
- Decision-making processes for IT-related decisions may be complicated or lack clarity due to the IT operating model's complexity.
- Incredibly high IT expenses

5. **The landscape of threats in which the company operates.**

   All enterprises in the financial industry sector have a high-threat environment.

6. **Compliance requirements to be met by the company.**

   All financial organizations in Jordan are subjected to higher-than-average compliance requirements.

7. **The role of IT in the company.**

   IT in the bank is critical for both running and innovating the organization's business processes and services.

8. **Company acquisition model (outsource, cloud, insource, hybrid,…)**

   The bank implants an onsite team from within their existing workforce to carry out IT tasks instead of outsourcing the same to a third party. As part of its insourcing strategy, businesses train and upskill internal employees to perform tasks. However, they have some outsourcing systems and Microsoft 365 cloud services.

9. **IT implementation method (agile, DevOps,traditional, hybrid)**

   In the bank, the IT implementation method focuses on prioritization of customer satisfaction and adaptability during software development.

10. **Technology adoption strategy**

    The bank technology adoption strategy is akin to stepping onto the frontlines of innovation. they believe that early adoption gains coveted advantages, leveraging technological superiority to outpace competitors, secure a larger market share, and reap higher economic profits. However, this pioneering path is not without its challenges – substantial initial investments, the spectrum of technological uncertainty, and the risk of others mimicking the adoption at a lower cost.

11. **Company size**

    Over 700 full-time employees (FTEs).

As Information Security Manager. Your job is required to work with a global IT and business team. The role will assist in defining, creating, and managing information security and organizational policies and standards in support of legality. Your Managing Director asked to provide a detailed report and a design factor study including the following tasks to share with the global IT team.

Part 1

1. Examine the key principles of an ISMS and its relevance to the successful operation of an organisation.
2. Analyse the benefits an effective ISMS can have on an organisation.
3. Critically analyse what is required to establish and maintain an ISMS for a selected organisation, ensuring that the key principles are met. (Note: your answer must be detailed as research)
4. Assess the elements (components) and processes required to establish and maintain an ISMS.
5. Justify the steps required for implementing an ISMS for a selected organisation.

Part 2

1. Based on business requirements plan the design of an ISMS for a selected organisation including an implementation map.
2. Appraise the planned ISMS designed, against the organisational requirements.
3. Justify the planned ISMS design for a selected organisation by following the stages of the audit.
4. Recognise the purpose of the international ISMS standards.
5. Analyse the relationship between standards and\ establishing an effective ISMS in an organisation.
6. Critically examine the advantages and disadvantages of the planned ISMS against the key international standards. in the context of its strengths and shortcomings and suggest appropriate corrective measures (remedies that might be taken) to improve its effectiveness. (Note: your answer must be detailed as research)

Learning Outcomes and Assessment Criteria			
Learning Outcome	**Pass**	**Merit**	**Distinction**
LO1 Explore the basic principles of information security management.	**P1** Examine the key principles of an ISMS and its relevance to the successful operation of an organization.	**M1** Analyze the benefits an effective ISMS can have on an organization.	**D1** Critically analyze what is required to establish and maintain an ISMS for a selected organization, ensuring that the key principles are met.
LO2 Critically assess how an organization can implement and maintain an Information Security Management System (ISMS).	**P2** Assess the elements and processes required to establish and maintain an ISMS.	**M2** Justify the steps required for implementing an ISMS for a selected organization.	
LO3 Appraise an ISMS and describe any weaknesses it may contain.	**P3** Plan the design of an ISMS for a selected organization, including an implementation map. **P4** Appraise the planned ISMS designed, against the organizational requirements.	**M3** Justify the planned ISMS design for a selected organization by following the stages of audit.	**D2** Critically examine the advantages and disadvantages of the planned ISMS against the key ISO and international standards.
LO4 Examine the strengths and weaknesses of implementing ISMS standards.	**P5** Recognize the purpose of the key ISO and international ISMS standards.	**M4** Analyze the relationship between ISO standards and\ establishing an effective ISMS in an organization.	