ASSIGNMENT BRIEF

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

Student Name/ID Number/Section	
HTU Course Number and Title	10203300 Information Security Management
BTEC Unit Code and Title	
Academic Year	2024-2025 2
Assignment Author	Hazem Arabiyat
Course Tutor	Hazem Arabiyat
Assignment Title	SecureLink Insurance Services
Assignment Ref No	1
Issue Date	21/04/2025
Formative Assessment dates	From 11/05/2025 to 29/05/2025
Submission Date	07/06/2025
IV Name & Date	Isra' Hasan 20/04/2025

Submission Format

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

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 are required to use the **ISACA toolkit** in their work.
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. The report should include a **cover page**, **table of contents**, and an **introduction** to provide an overview of the content.
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**.

Notes:

- If you do not see the **Turnitin report** when you initially submit your report, contact your instructor immediately.
- **Resubmission:** If you lose more than **3 Pass criteria (Ps)**, you will **NOT be eligible** for resubmission.

Submission:

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

Case Study Synopsis:

We will be using SecureLink Insurance Services as an exemplar model in this Information Security Management System (ISMS) project assignment. SecureLink is a rapidly growing, fully digital insurance company headquartered in Amman , with regional offices in Dubai and Riyadh. The company offers a range of insurance products such as:

- Cyber insurance
- Health insurance
- Property insurance

SecureLink operates through cloud services (AWS) and integrates AI-based fraud detection. The Managing Director (MD) has decided to design and implement COBIT 2019 to address growing compliance and risk management challenges. The organization recognizes that such a decision is critical to meet business needs and comply with various international regulations.

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

1. The Strategy of the Company

- Embrace digital transformation.
- Build trust with customers.
- Innovate insurance solutions.
- Maintain strong employee culture.
- Prioritize remote work strategies.
- Accelerate cloud adoption and automation.

2. Company Goals Supporting the Strategy

- Maximize profits
- Launch new insurance products
- Improve customer service
- Increase operational efficiency
- Establish industry leadership
- Expand market share in MENA and Europe
- Boost social media presence
- Implement employee recognition programs

3. The IT Risk Profile of the Company

Risk Description	Impact Area	Impact Value	Probability	Impact Severity
Phishing targeting policyholder data	Reputation/Goodwill	3	High	Medium
Ransomware attack on cloud environment	Cash/Legal	4	Medium	High
Third-party vendor data breach	Reputation/Goodwill	3	Medium	Medium
Weak password policies	Reputation/Goodwill	2	High	Low
Insider threat (employee leaking data)	Reputation/Goodwill	2	Low	High
Cloud storage misconfiguration	Cash/Profitability	3	Medium	High
AI fraud detection system failure	Reputation/Goodwill	2	Low	High
DDoS attack on insurance services portal	Reputation/Goodwill	3	Medium	Medium
Delays in claim processing system updates	Cash/Profitability	4	High	Medium
Insecure API integrations with partners	Cash & Legal	3	Medium	High
GDPR non-compliance penalties	Cash & Legal	2	Low	High
Delay in cloud security patches	Reputation/Goodwill	3	Medium	High
Mobile app vulnerabilities	Reputation/Goodwill	3	Medium	Medium
Slow incident response times	Reputation/Goodwill	4	High	Medium

Ineffective cloud resource monitoring	Reputation/Goodwill	3	Medium	Medium

4. I&T Risks or Issues Already Materialized

- Communication gaps between IT specialists and business units.
- Complex IT operating model delays decision-making.
- High IT operational costs.
- Past delays in vendor security compliance.

5. Threat Landscape

Operating in a high-risk environment typical of the financial industry. Frequent targeting by ransomware and phishing attacks.

6. Compliance Requirements

- GDPR (EU regulation)
- Local data protection laws in UAE, Saudi Arabia, and Jordan.
- PCI-DSS for payment data security.

7. The Role of IT

IT is essential for both operations and innovation. Supports customer portals, AI risk models, and cloud infrastructure.

8. Company Acquisition Model

Hybrid model: Primarily insourced IT team with some outsourced systems and Microsoft 365 cloud services.

9. IT Implementation Method

Agile/DevOps: Focused on customer satisfaction, flexibility, and fast iteration.

10. Technology Adoption Strategy

Early adoption for competitive advantage. Balancing high initial investments and fast technological evolution.

11. Company Size

Over 300 full-time employees (FTEs).

As the Information Security Manager, your role involves:

Working closely with the global IT and business team to define, create, and manage the company's information security and organizational policies. Your Managing Director has tasked you with delivering a comprehensive report and design factor study, covering:

Part 1

- Critically analyse what is required to establish and maintain an ISMS for SecureLink. (Detailed research required.)
- Assess the elements and processes required to establish and maintain an ISMS.
- Justify the steps required for implementing an ISMS for SecureLink.

Part 2

- Plan the design of an ISMS for SecureLink, including an implementation map.
- Appraise the planned ISMS design against the organization's requirements.
- Justify the ISMS design by following the audit stages.
- Recognize the purpose of international ISMS standards.
- Analyse the relationship between standards and establishing an effective ISMS.
- Critically examine the advantages and disadvantages of the planned ISMS compared to international standards. (Detailed research required.)

part 3: In-Class Exam

- The in-class written exam covers the following assessment criteria:
  - **P1 –** Examine the key principles of an ISMS and its relevance to the successful operation of an organisation.
  - **P5 –** Recognise the purpose of the key ISO and international ISMS standards.
  - **M1 –** Analyse the benefits an effective ISMS can have on an organisation.

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 organisation.	**M1** Analyse the benefits an effective ISMS can have on an organisation.	**D1** Critically analyse what is required to establish and maintain an ISMS for a selected organisation, 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 organisation.	
LO3 Appraise an ISMS and describe any weaknesses it may contain.	**P3** Plan the design of an ISMS for a selected organisation, including an implementation map. **P4** Appraise the planned ISMS designed, against the organisational requirements.	**M3** Justify the planned ISMS design for a selected organisation 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** Recognise the purpose of the key ISO and international ISMS standards.	**M4** Analyse the relationship between ISO standards and\ establishing an effective ISMS in an organisation.	