

**QUALIFI ASSESSMENT DOCUMENT**

|  |  |
| --- | --- |
| Qualification Unit Name |  **SEM205IT Cyber Security** |
| Unit Reference |  A/650/1915 |
| No of Credits | 10 Credits |

Contents

[Introduction 2](#_Toc198665806)

[Assignment Guidelines 2](#_Toc198665807)

[Plagiarism and Collusion 2](#_Toc198665808)

[Appendices 2](#_Toc198665809)

[Confidentiality 3](#_Toc198665810)

[Word Count Policy 3](#_Toc198665811)

[Marking and grades 3](#_Toc198665812)

[Learning Outcomes and Assessment Criteria 4](#_Toc198665813)

[Referencing and Professionalism 5](#_Toc198665814)

[Submission of Assignments 5](#_Toc198665815)

[ASSESSMENT TASKS 6](#_Toc198665816)

[Task 1 FORMATIVE TASK Cybersecurity in Principle 6](#_Toc198665817)

[Task 2 SUMMATIVE TASK Cybersecurity within your Organisation 7](#_Toc198665818)

[Mark Scheme 8](#_Toc198665819)

[Instructor’s Comments 8](#_Toc198665820)

[Qualifi Information 10](#_Toc198665821)

Introduction

Prior to attempting this coursework assignment, Learners must familiarise themselves with the following policies:

* Centre Specification
* Qualifi Quality Assurance Standards
* Qualifi Quality Policy Statement

Assignment Guidelines

All work must be submitted in a single electronic document (.doc/.docx file). The assignment must be the Learner’s own work and not copies of theories or models. Direct quotes should be kept to a minimum and shown in inverted commas. Models described and other quotes used must be properly attributed and referenced as appropriate. Learners must acknowledge or reference any sources that have been used to complete the assignment, listing reference material and websites used.

Plagiarism and Collusion

In submitting the assignment Learners must complete a statement of authenticity confirming that the work submitted for all tasks is their own. The statement should also include the word count. Plagiarism and collusion are treated very seriously. Plagiarism involves presenting work, excerpts, ideas or passages of another author without appropriate referencing and attribution. Collusion occurs when two or more learners submit work, which is so alike in ideas, content, wording and/or structure that the similarity goes beyond what might have been mere coincidence.

Appendices

Separate Appendices should not be used. Any use of tables, graphs, diagrams, Gantt chart and flowcharts etc. that support the main report should be incorporated into the back of the assignment report that is submitted. Any published secondary information such as annual reports and company literature, should be referenced in the main text of the assignment but not included.

Confidentiality

Where a Learner is using organisational information that deals with sensitive material or issues, they must seek the advice and permission from that organisation about its inclusion. Where confidentiality is an issue, Learners are advised to anonymise their assignment report so that it cannot be attributed to that particular organisation.

Word Count Policy

In total, the assignment should be between 1850 – 2150 words. Learners must comply with the required word count, within a margin of +10%.These rules exclude the index (if used), headings and information contained within references and bibliographies. When an assessment task requires learners to produce presentation slides with supporting notes, the word count applies to the supporting notes only.

Marking and grades

Qualifi uses a standard marking rubric for all assignments, and you can find the details at the end of this document.

Unless stated elsewhere, Learners must answer all questions in this document.

|  |  |
| --- | --- |
| **Unit Title** | Cyber Security |
| **Unit Reference (RQF)** | A/650/1915 |
|  **No of Credits** | 10 |

Learning Outcomes and Assessment Criteria

|  |  |
| --- | --- |
| **Learning Outcomes**When awarded credit for this unit, a student will: | **Assessment Criteria**Assessment of this learning outcome will require a student to demonstrate that they can: |
| 1. Understand cyber security. | * 1. Describe the concepts of cyber security.
	2. Explain the importance of cyber security for businesses.
	3. Describe the consequences and implications of inadequate cyber security for businesses .
 |
| 2. Understand core terminology and key aspects of cyber security. | * 1. Define core terminology used in cyber security.
	2. Compare typical behaviors of good actors and bad actors.
	3. Analyse the sectors that are most vulnerable to a cyber-attack.
 |
| 3. Understand cyber threat intelligence. | * 1. Identify the concepts of cyber threat intelligence
	2. Explain the following terms in relation to cyber security:
		+ threats
		+ exploits
* risks
* vulnerabilities

 3.3 Identify improvements to secure a network against cyber-attacks. |

Referencing and Professionalism

A professional approach to work is expected from all learners. Learners must therefore identify and acknowledge ALL sources/methodologies/applications used. The learner must use an appropriate referencing system to achieve this. Marks are not awarded for the use of English; however the learner must express ideas clearly and ensure that appropriate terminology is used to convey accuracy in meaning.

Submission of Assignments

All work must be submitted in a single electronic document (.doc/.docx file) in your Learning Portal or to submit to the Assessor/Centre Administrator.

ASSESSMENT TASKS

Task 1 FORMATIVE TASK Cybersecurity in Principle

**FORMATIVE TASK**

Instruction: What does cybersecurity mean for organisations in your market sector? Write a report to explain this issue to a group of non-specialists. Your report must include the following:

* An outline of the principle of cybersecurity in general terms
* Identify and explain the importance of cyber security for your market sector
* Discuss the consequences and implications of inadequate cyber security within your organisation

**Formatting**:

450-550 words

Justified alignment

Single-spaced

12pt Times New Roman font

Use an appropriate referencing system for footnotes and citations

Task 2 SUMMATIVE TASK Cybersecurity within your Organisation

**SUMMATIVE TASK**

Instruction: Undertake a case study of cybersecurity within an organisation of your choosing. Your report on the case study must contain the following:

* An outline of the core terminology used, and how threats to the organisation are identified (LO 2.1, 3.1)
* Identify and explain how bad actors bring threats, exploits, risks and vulnerabilities to the cybersecurity of the organisation (LO 2.2, 3.2)
* A judgment as what needs to be done next to ensure the cybersecurity of the organisation as a whole (LO 2.3, 3.3)

|  |  |
| --- | --- |
| **Learning Outcomes**When awarded credit for this unit, a student will: | **Assessment Criteria**Assessment of this learning outcome will require a student to demonstrate that they can: |
| 2. Understand core terminology and key aspects of cyber security. | * 1. Define core terminology used in cyber security.
	2. Compare typical behaviors of good actors and bad actors.
	3. Analyse the sectors that are most vulnerable to a cyber-attack.
 |
| 3. Understand cyber threat intelligence. | * 1. Identify the concepts of cyber threat intelligence
	2. Explain the following terms in relation to cyber security:
		+ threats
		+ exploits
* risks
* vulnerabilities

 3.3 Identify improvements to secure a network against cyber-attacks. |

**Formatting**:

1450-1550 words

Justified alignment

Single-spaced

12pt Times New Roman font

Use an appropriate referencing system for footnotes and citations

**Learners are required to complete all tasks.**

Mark Scheme



Instructor’s Comments

|  |
| --- |
|  |

**Marking Directions:**

1. For each of the criteria listed in the first column, circle one box in the corresponding column to the right, which best reflects the student’s work on this particular assessment activity (e.g., project, presentation, essay).
2. Provide specific feedback to a student about each of the criteria scores he/she earned by writing comments and suggestions for improvement in the last row titled “Instructor’s comments.”
3. To arrive at a mark, total the boxes and divide by 5 to arrive at a final mark

Example:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Distinction** | **Merit** | **Pass** | **Fail** |
| **Range** | 70-100 | 60-69 | 40-59 | 0-39 |

|  |  |
| --- | --- |
| **Criteria** | **Score** |
| Content | 50 |
| Application of Theory and Literature | 40 |
| Knowledge and Understanding | 50 |
| Presentation/Writing Skills | 40 |
| Referencing | 40 |
| **Total Score** | 220/5 = **44, Pass** |

Qualifi Information

**HEAD OFFICE**

Qualifi Ltd.

Fairways House

George Street

Prestwich

Greater Manchester

M25 9WS

Copyright 2025 Qualifi Ltd