


SEVERN BUSINESS COLLEGE

# Qualifi Level 7 Diploma in Cyber Security

Course Handbook

### Qualification
Qualifi Level 7 Diploma in Cyber Security

### Ofqual Number
610/3596/8

### Level
7

### Total Qualification Time
1200

### Credit Value
120

### Aim of the Course
The aim of the Qualifi Level 7 Diploma in Cyber Security is to offer learners an advanced knowledge of the industry by deepening their awareness of cyber threats, vulnerabilities, and security technologies. The core objective of the Qualifi Level 7 Diploma in Cyber Security qualification is to equip learners with the underpinning knowledge, understanding and skills required for a career in the cyber security sector.

### Assessment
Assessment is through practical assignments, with no exams - to more accurately reflect the real working environment.

### Course Structure

| **Qualifi Level 7 Diploma in Cyber Security** | | | |
|---|---|---|---|
| **Unit number** | **Units** | **Unit level** | **Unit credit** |
| H/650/9532 | Fundamentals of Cyber Security | 7 | 20 |
| J/650/9533 | Network, Infrastructure and Systems Security | 7 | 20 |
| K/650/9534 | Applications of Cyber Security | 7 | 20 |
| L/650/9535 | Security Management and Governance | 7 | 30 |
| J/617/4634 | Cryptography | 7 | 30 |

### Assessment Grades

| **Grade** | **Marking Criteria** |
|---|---|
| Pass | All learning outcomes are achieved. All assessment criteria are met. |
| Fail | All learning outcomes are not achieved. All assessment criteria are not met. |
| No Marks | Plagiarism |

## UNIT SPECIFICATIONS

### Unit Title
Fundamentals of Cyber Security Technology

### Level
7

### Learning Time Hours
200

### Credit Value
20

### Unit aim
The aim of this unit is to give learners an understanding if the key concepts of cyber security, allowing them to recognise and analyse security threats in a range of scenarios.

### Learning outcomes and assessment criteria
In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

| **Learning Outcome** | **Assessment Criteria** |
|---|---|

| | |
|---|---|
| 1. Understand the key concepts in cyber security. | 1.1 Discuss what is meant by cyber security and its importance.<br>1.2 Analyse the principal techniques and technologies used to achieve cyber security and the challenges faced. |
| 2. Understand the impact of cyber security threats and attacks on individuals and organisations. | 2.1 Analyse existing and emerging threats and the impact on individuals and organisations.<br>2.2 Discuss the organisational policies and procedures that need to be in place to protect against cyber security attacks.<br>2.3 Analyse how organisations can stay up to date with shifting cyber security threats and protect their operations and data. |

### Suggested Resources

- Fundamentals of Cybersecurity [The Basics Guide]. (n.d.). https://www.knowledgehut.com/blog/security/cyber-security-fundamentals
- Shea, S., Gillis, A. S., & Clark, C. (2023, January 11). What is cybersecurity? Security. https://www.techtarget.com/searchsecurity/definition/cybersecurity

## UNIT SPECIFICATIONS

### Unit Title
Network, Infrastructure and Systems Security

### Level
7

### Learning Time Hours
200

### Credit Value
20

### Unit aim
The main objective of this unit is to for learners to gain an understanding of the various types of threats and vulnerabilities that can affect computer networks, infrastructure and systems, such as malware, hacking, and social engineering. It also aims to familiarise learners with various security technologies and tools, such as firewalls, intrusion detection systems, and encryption methods.

### Learning outcomes and assessment criteria
In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

| Learning Outcome | Assessment Criteria |
|---|---|
| 1. Understand the security implications of networked systems. | 1.1 Discuss the concepts and the role of<br>• Network types<br>• Network components<br>• Networking infrastructure services and resources.<br>1.2 Analyse network security protection methods |
| 2. Understand the design and security of an organisational network. | 2.1 Analyse operational technologies, the internet and critical infrastructure.<br>2.2 Evaluate vulnerabilities and exploits that target computer networks and systems, the internet infrastructure.<br>2.3 Assess approaches to modelling, assessing and testing networks and systems.<br>2.4 Review access controls on a cyber-security network system and make recommendations as appropriate. |
| 3. Understand networking topologies and how to secure them. | 3.1 Explore that the different elements that affect network performance.<br>3.2 Analyse present and future cyber security and information security technologies.<br>3.3 Evaluate the strengths and weaknesses of a network for a given organisation in relation to cyber security. |
| 4 Understand computer systems from the operating systems and security services | 4.1 Evaluate a range of deployments that support the worldwide web and distributed computing services. |

### Suggested Resources

- What is Network Security? The Different Types of Protections. Check Point Software.

https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/
- Network and System Security. (n.d.). ScienceDirect. https://www.sciencedirect.com/book/9780124166899/network-and-system-security
- Network Security. (2023, March 21). GeeksforGeeks. https://www.geeksforgeeks.org/network-security/

## UNIT SPECIFICATIONS

### Unit Title
Applications of Cyber Security

### Level
7

### Learning Time Hours
200

### Credit Value
20

### Unit aim
The aim of this unit is to for learners to learn about the security measures and defence mechanisms that are used to defend against and respond effectively to security incidents, breaches, and anomalies.

### Learning outcomes and assessment criteria
In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

| Learning Outcome | Assessment Criteria |
|---|---|
| 1. Understand the principles around software and applications. | 1.1 Analyse the issues of malicious software and the effect on the security of systems.<br>1.2 Evaluate physical and infrastructure security measures to defend against attacks and threats.<br>1.3 Explore defence mechanisms, host and application security. |
| 2. Understand the techniques used for secure software development. | 2.1 Discuss principles of secure programming.<br>2.2 Explain common software vulnerabilities that can be introduced during software development.<br>2.3 Analyse aspects of mobile and cloud security.<br>2.4 Explore wider considerations and research directions for software and application security. |

### Suggested Resources
- Incident Response | Cyber Security Incident Response Services. (2023, October 9). Redscan. https://www.redscan.com/services/cyber-incident-response/
- Wall, P. (2023, October 17). Define Your Incident Response Lifecycle | Application Security | Imperva. Learning Center. https://www.imperva.com/learn/application-security/define-security-incident-response/
- Beaver, K. (2023, February 23). Top incident response tools: How to choose and use them. Security. https://www.techtarget.com/searchsecurity/feature/Incident-response-tools-How-when-and-why-to-usethem

## UNIT SPECIFICATIONS

### Unit Title
Security Management and Governance

### Level
7

### Learning Time Hours
300

### Credit Value
30

### Unit aim
The aim of this unit is to develop learners understanding of what constitutes effective security management in relation to different types of cyber threat that can affect organisations and individuals. Learners will have the opportunity to analyse and review a response to a cyber security incident.

### Learning outcomes and assessment criteria
In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

| Learning Outcome | Assessment Criteria |
|---|---|
| 1. Understand the need for effective security management. | 1.1 Critically review the main currently used approaches to management, including key standardised approaches and the fundamental importance of a risk-based approach. |
| 2. Understand key components of practical cyber security management. | 2.1 Discuss key related legislation and regulations and the impact on security management and importance for organisations to continuously monitoring their compliance.<br>2.2 Analsye the importance of auditing in a security management context.<br>2.3 Assess key role of people in achieving robust cyber security.<br>2.4 Develop strategies to integrate a range of possible information security technologies and techniques into a security management system for a given organisation. |
| 3: Understand how to respond to a cyber security incident effectively and the appropriate chain of events. | 3.1 Explain the reporting processes involved in responding to a cyber security incident.<br>3.2 Discuss the documentation that needs to be produced and maintained during and after a cyber security incident, including future actions.<br>3.3 Analyse how to ensure business continuity during a cyber security incident. |

### Suggested Resources
- Cyber Security Threats and Countermeasures. Social Science Research Network; RELX Group (Netherlands). https://doi.org/10.2139/ssrn.4425678
- Security Threats and Countermeasures | Global | Ricoh. (n.d.). Copyright RICOH Co., Ltd. https://www.ricoh.com/products/security/mfp/countermeasur

## UNIT SPECIFICATIONS

### Unit Title
Cryptography

### Level
7

### Learning Time Hours
300

### Credit Value
30

### Unit aim
The aim of this unit is for learners to develop their understanding of cryptography, the different cryptography tools and how and when these tools are used.

### Learning outcomes and assessment criteria
In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria determine the standard required to achieve the unit.

| Learning Outcome | Assessment Criteria |
|---|---|
| 1: Understand the key concepts of cryptography and its limitations. | 1.1 Analyse how the security of everyday digital applications tools is achieved and maintained.<br>1.2 Explain the concepts of confidentiality and data integrity.<br>1.3 Analyse the wider infrastructure surrounding cryptography and how this impacts the overall security of systems deploying cryptography. |

| | |
|---|---|
| 2: Understand the function and purpose of the main cryptographic tools. | 2.1 Explain how the main cryptographic tools are used. Assess the decision-making process used to select the most appropriate cryptographic tools to deploy in specific settings. |

### Suggested Resources

- Data Backup & Recovery | Certitude Security | Cyber Security. (2023, February 10). Certitude Security. https://www.certitudesecurity.com/services/data-backup-and-recovery/
- Cybersecurity Risk Management | Frameworks, Analysis & Assessment | Imperva. Learning Center. https://www.imperva.com/learn/data-security/cybersecurity-risk-management/
- What is Cybersecurity Risk Management? Preventing Cyber Attacks | Up Guard. (n.d.). https://www.upguard.com/blog/cybersecurity-risk-management

Version:2507a