Certificate in Cyber Security Practices L3

Contents

What is this Qualification?

The NCFE Level 3 Certificate in Cyber Security Practices is a regulated qualification designed to provide learners with knowledge and skills relating to cyber security practices.

Key aims and objectives of this course are:

- To provide the learner with an opportunity to develop knowledge and skills relating to cyber security practices.
- To focus on the study of the practices within cyber security.
- To offer breadth and depth of study, incorporating a key core of knowledge.
- To provide opportunities to acquire a number of practical skills.
- This qualification is at **Level 3**.

Who is this Course for?

Prior Knowledge and Suitability:

- There is **no specific prior knowledge** a learner must have to start this qualification.
- However, learners will need to have **good written and spoken English** to successfully complete the course assessments. Learners may also find it helpful if they have previously achieved a Level 2 Digital Skills or Information Technology qualification.

Why Should Learners Enrol?

- **This course offers:**
  - A strong foundation in cyber security principles.
  - Knowledge of current threats and how to respond to them.
  - Awareness of legal and ethical responsibilities.
  - Development of professional behaviours and career planning.
- **Skills gained include:**
  - Identifying and analysing cyber threats.
  - Understand how to test systems and applying security controls.
  - Responding to incidents and writing reports.
  - Understanding legislation and ethical conduct.
  - Building a personal development plan for career growth.

Guided Learning Hours & Commitment

- **GLH:** 150 hours (taught sessions)
- **Total Qualification Time (TQT):** 220 hours (includes independent study)
- Learners should expect to commit additional time outside of lessons for:
  - Research
  - Assignments
  - Portfolio building

Unit Breakdown

Unit 01: Understand cyber security principles (30 GLH)
Learners will gain an understanding of fundamental concepts and actors in cyber security.

- Core Concepts: You must define and understand terms like confidentiality, integrity, availability, threat, vulnerability, risk, and hazard. Other required terminology includes malicious software, Distributed Denial of Service (DDoS), exploit, breach, firewall, encryption, Bring Your Own Device (BYOD), and penetration testing (pen testing).
- Consequences of Inadequate Security: Must cover implications such as the unauthorised access, distribution, or loss of sensitive data, Personally Identifiable Information (PII), Protected Health Information (PHI), intellectual property, and industry information systems.
- Actors and Motivations: You will distinguish between 'good actors' (e.g., white hat hackers, certified penetration testers) and 'bad actors' (e.g., ex-employees, black hat hackers, hacktivists, script kiddies). Motivations covered for bad actors include

financial gain, terrorism, political motivation, and disruption, while good actor motivations include ethical reasons, job roles, and innovation.
- Security by Design: You will evaluate the advantages and disadvantages of security by design and explore its principles, potentially using guidelines from organisations like the National Cyber Security Centre (NCSC).

Unit 02: Threat intelligence in cyber security (30 GLH)
This unit focuses on identifying and analysing potential threats.
- Threat Intelligence: You will explore the threat intelligence lifecycle and the importance of using reliable and valid sources of Open Source Intelligence (OSINT) data.
- Malicious Software: You must identify and describe the effects of various malicious software types, including virus, spyware, trojan, and worms.
- Threat Models: You are required to describe a minimum of three threat models. Examples provided include STRIDE (Spoofing, Tampering, Repudiation, etc.), PASTA (Process for Attack Simulation and Threat Analysis), LINDDUN, CVSS (Common Vulnerability Scoring System), and Attack Trees.
- Social Engineering: You will explore how OSINT can be used to facilitate social engineering attacks.

Unit 03: Cyber security testing, vulnerabilities and controls (30 GLH)
- This unit focuses on practical testing, remediation, and control application.
- Testing Types: You will learn about different types of cyber security testing, including penetration testing, vulnerability testing, and social engineering testing. You must also consider mitigations following testing, such as escalation, software/OS updates, user access control, and staff training and awareness.
- Vulnerability Response: You must demonstrate the steps to be taken when a vulnerability is identified, including reference to organisational policies/procedures. Appropriate responses may include patching or carrying out an update.
- Controls and Frameworks: You are required to explain a basic cyber security framework, such as the NCSC 10 Steps to Cyber Security or the Centre for Internet Security (CIS) controls.
- Practical Skill: You must implement a basic cyber security control (e.g., demonstrating how to give or deny access to a folder or drive) and justify its implementation.

Unit 04: Cyber security incident response (30 GLH)
This unit covers the necessary steps for managing and reviewing security breaches.
- Incident Response Plan: You must describe the use and stages of a cyber security incident response plan, including the incident response lifecycle. The plan often contains a vital checklist.

- Incident Log and Post Mortem: You will learn why it is important to maintain an up-to-date incident log. You will also cover how to create an incident post mortem report. When carrying out a post mortem, you must understand the importance of integrity, rigour, and discipline. You may be provided with a case study of a medium to large-scale incident to develop this report.

Unit 05: Understand legislation and ethical conduct (20 GLH)
This unit focuses on the legal, ethical, and standards environment surrounding cyber security.

- Key Legislation: You must describe how a minimum of four pieces of legislation impact cyber security. Examples include the Computer Misuse Act 1990, the Official Secrets Act 1989, the Data Protection Act 2018/UK General Data Protection Regulation (UK GDPR), and the Police and Criminal Evidence Act 1984 (PACE). You must cover current and relevant legislation.
- Information Security Standards: You must identify and explain how information security standards, such as ISO/IEC 27001:2013 or ISO/IEC 27032:2012, support cyber security.
- Ethical Conduct: You must cover required ethical conduct (e.g., maintaining confidentiality, adherence to applicable laws, promoting information security) and identify specific unethical conduct (e.g., sabotage, disclosing or misusing confidential information).

Unit 06: Professional skills and behaviours (10 GLH)
This unit covers the essential professional readiness required for a career in the industry.

- Digital Identity: You must explain the importance of managing and promoting a positive digital identity, noting that a digital image or footprint can be traced and used by third parties like employers.
- Screening and Clearance: You will describe potential employee screening checks, which must include a Disclosure and Barring Service (DBS) check, security checks (terror lists, address checks), credit checks, and a guilty by association check. You will also describe three security clearance levels: BPSS (Baseline Personnel Security Standard), SC (Security Checked), and DV (Developed Vetting).
- Personal Development: You will perform a personal skills analysis (potentially using methods like SWOT or SOAR). Based on this analysis, you must create a Personal Development Plan (PDP) that addresses areas for growth using SMART targets. You must also explain Continuous Professional Development (CPD) and its importance.

Assessment Method

- Learners will be assessed through a **portfolio of evidence** (6 workbooks, one for each unit), which includes:
    - Written reports
    - Presentations
    - Discussions
    - Assignments
    - Case studies
- All assessments are:
    - **Internally assessed** by tutors.
    - **Externally quality assured** by NCFE.

Career Pathways

After completing the course, learners can progress to:

- Level 4 qualifications in cyber security or IT.
- Entry-level roles such as:
    - First Line IT Support
    - Cyber Security Technician
    - IT Support Analyst
    - SOC (Security Operations Centre) Analyst
    - Junior Penetration Tester