



TLM Level 2 Award in Cyber Security Awareness

The TLM Level 2 Award in Cyber Security Awareness has been developed in direct response to employer demand following a series of high-profile cyber incidents across the UK. It equips non-specialist staff and team leads with the essential principles of organisational cyber security, emphasising that effective defence is everyone's responsibility and that people, as much as technology, shape an organisation's resilience.

Learners will explore how common attacks exploit human behaviour—particularly social engineering—and how straightforward, repeatable actions reduce risk. They will learn to recognise typical threat patterns, apply safe working practices (such as strong pass-phrases and multi-factor authentication), follow local policies for reporting concerns, and act as a first point of escalation for their teams. Throughout, the programme aligns with recognised UK good practice and encourages clear communication, good record-keeping, and a positive security culture.

By the end of the course, learners can identify and respond to everyday cyber risks with confidence, support colleagues to do the right thing, and contribute to incident reporting and recovery in line with organisational procedures. This qualification provides a concise, practice-focused foundation for those progressing to further study in cyber security or digital support at Level 3, and for employees taking on 'staff champion' responsibilities within their workplace.

This qualification has been developed in consultation with Sparks, a company specialising in embedded systems, smart IoT technologies with Artificial Intelligence, and software development. Their insight into industry needs and current technical practices has helped ensure that the qualification content reflects the real-world skills, tools, and challenges learners are likely to encounter in operational and development roles within the embedded systems sector.



Table of Contents

1. For those in a hurry!	4
2. Introduction	5
3. Summary of Qualification Specification	6
4. Qualification Content	7
5. Support	8
6. Registration & Procedures	9
7. Other Considerations	10
Annexe A	11
Level 2 Award in Cyber Security Awareness - Unit assessment - coursework guidance	11
Accessibility Policies	12
CASLO Approach	13

1. For those in a hurry!

- 1.1** TLM's assessment model is common to most of its qualifications. It is based on competence-based assessment of coursework using a portfolio of evidence and supported by a free optional cloud-based evidence management system.
-

- 1.2** Learners must demonstrate competence against the assessment criteria from their day-to-day work and the tutor assessor must verify that they are competent in relation to the general level descriptor using indicative assessment criteria.

TLM's external moderator will check the judgements and the quality of the evidence and provide feedback. This process is not graded, the intention is that it is a flexible way of checking basic practical competence in the subject at the qualification's framework level.

Procedures

- 1.3** The first thing to do is to arrange assessor training with TLM. TLM trains at least one assessor as Principal Assessor who must accept responsibility for standards within the Centre. The Principal Assessor can train and appoint assessors within the Centre as long as they are competent to take on the work and are willing to sign an agreement on the web site to uphold standards.
-

- 1.4** TLM will provide initial training in the pedagogical model, and using the supporting technologies to provide the evidence needed. The purpose is to get you started and then we provide on-going support to ensure you are confident and we can work as a professional partnership.

We advise new Centres to do some coursework assessment early so that they can receive feedback and quickly become confident in doing routine coursework assessment. Our aim is to make this no more onerous than normal routine assessment that anyone would do as a normal part of the teaching job. This gives more time to focus on teaching and therefore to support raising attainment.

2. Introduction

This Level 2 Award in Cyber Security Awareness is designed to introduce learners to the essential principles of organisational cyber security and the human factors that influence it. Learners will explore how common threats—particularly social engineering—are constructed and detected, practise everyday protective behaviours such as strong pass-phrases, multi-factor authentication and secure data handling, and learn how to report concerns promptly in line with local policy.

The programme frames risk using the confidentiality–integrity–availability (CIA) model and signposts recognised UK guidance (for example, NCSC’s Cyber Aware and Cyber Essentials) so that good practice can be applied in real workplace settings.

The qualification provides a strong foundation for those seeking to act as staff cyber-hygiene champions or to progress to further study in digital support and cyber security.

The Level 2 Award in will give learners the opportunity to:

- Engage in learning aligned to recognised UK good practice, developing the confidence to recognise threats, take appropriate action, and reinforce a positive security culture
- Achieve a nationally recognised Level 2 qualification
- Develop their own personal growth and engagement in learning.

2.1 TLM Level 2 Award in Cyber Security Awareness

The objective of the qualification is to provide learners with the knowledge and confidence to develop their own skills. This qualification includes optional units, and learners are required to complete a total of 15 credits in order to earn the qualification.

Mandatory Unit

- Unit 1 – Cyber Security Awareness – (2 Credits)

3. Summary of Qualification Specification

3.1 Level 2 Award (Annexe A)

This Level 2 Award in Cyber Security Awareness introduces learners to the human and organisational aspects of cyber security, developing practical skills in recognising threats, applying safe practices, and reporting incidents in line with recognised UK guidance.

Qualification Title: TLM Level 2 Award in Cyber Security Awareness

Qualification Number: XXX/XXXX/X

Qualification Level: Level 2

Total Credits: 2

Guided Learning Hours: 12

Total Qualification Time: 20

Assessment Methods: Coursework, E-assessment, Portfolio of Evidence

Assessment

Learners must demonstrate competence against the assessment criteria from their communication and involvement with the training materials and the trainer assessor must verify that they are competent in relation to the general level descriptor using indicative assessment criteria.

TLM's external moderator will check the judgements and the quality of the evidence and provide feedback. This process is not graded, the intention is that it is a flexible way of checking basic practical competence in the subject at the qualification's framework level.

CASLO review is shown on Page 13

3.2 Assessment

The internally assessed, externally moderated coursework for all qualifications is pass/fail but by submitting the evidence for external moderation, feedback can be given to the tutor on areas to improve for resubmission.

Evidence must be provided against the unit assessment criteria from practical tasks related to the learners' everyday work supported by tutor observations, portfolio completed, and or activities in line with the learning materials


The way evidence is gathered is up to the assessor, the only requirement is that it clearly supports the judgements against the assessment criteria and the relevant learning outcomes.

If on formative assessment the account manager finds gaps in evidence relating to a particular candidate, they will request more evidence before approving the award or the unit certificate. Assessors must then adjust their work to ensure all their learners are providing the appropriate level and breadth of evidence.

We encourage early submission of at least some evidence so that assessors are confident from the feedback that what they are providing is sufficient. In this way we can maintain standards while supporting improved efficiency.

Centres will be subject to the TLM Centre Assessment Standards Scrutiny (CASS) and further details of this, including our centre guidance, is freely available on the TLM website in our Policy Download Centre. <https://tlm.org.uk/policy-download-centre/>

4. Qualification Content

Mandatory	Optional Unit Bank
<div> Unit 1 – Cyber Security Awareness – (2 Credits)</div>	None

5. Support

Guidance and Assistance

- 5.1** There is further guidance for coursework assessment on the TLM web site. All centres have an assigned Account Manager who will be pleased to help at any time. Our aim is to give professional assessors, most of whom are qualified tutors, the confidence to make judgements with a minimum of bureaucracy so that they can focus their time on maintaining their professional knowledge, skills and supporting learning through effective teaching rather than “chasing paper”.

There is often a confusion between bureaucracy and rigour, since unnecessarily complex bureaucracy can actually detract from rigour by obscuring the importance of the outcomes.

- 5.2 Web sites** - TLM provides support through cloud-based systems. Providing assessment grades and the management of certification through the TLM Centre management system is mandatory and all assessors are provided with training in its use.

It is simply a matter of recording learner competence against the unit criteria as the evidence is collected and claiming a certificate on behalf of the learner when a unit has been fully assessed.

- 5.3** Use of the online community learning site is entirely optional. It offers a streamlined way for learners to submit evidence and for assessors and verifiers to manage feedback and tracking, reducing administrative workload for centres that choose to use it.
-

- 5.4 Telephone** and e-mail support are available to all Centres. There is a general convention of `firstname.secondname@tlm.org.uk` for e-mail addresses.
-

6. Registration & Procedures

Registration

- 6.1** TLM's registration model allows centres to enter learners at times convenient to them. There are no late entry fees and no additional fees should a learner fail to produce evidence at a level but can meet the criteria at a lower level. This can reduce costs to the centres when compared to other qualifications

There are no fees for replacement certificates or verification of certificates because all certificates can be directly authenticated against TLM's secure database.

Internal standardisation

- 6.2** The Principal Assessor has the ultimate responsibility for consistency in assessment standards within a centre. All assessors have signed a contract agreeing to uphold standards and should therefore co-operate with the Principal Assessor and Account Manager at TLM to ensure that standards across the centre are consistent.

It is advisable to send work samples to TLM early to check that evidence is at the right standard so that there is time to make any adjustments necessary to the course and learner expectations. TLM will generally check a higher quantity of work from new assessors and feedback to ensure that they are confident to make appropriate judgements over time. This reduces risk and improves efficiency in the longer term.

Authentication

- 6.3** All assessors must take reasonable steps to ensure that any coursework evidence submitted by candidates is a true reflection of the candidates' competence. This is in keeping with the assessor undertaking to uphold and maintain standards in the contract with TLM.
- 6.4** Certificates can be easily authenticated online by entering the certificate number or scanning the QR code printed on the certificate.

This service is free of charge and encourages routine verification, which helps strengthen overall security.

When authentication is not quick and accessible, the risk of certificate fraud increases significantly.

With the growing sophistication of technologies—especially AI-powered image generation—creating highly convincing forgeries is becoming easier and more common, making robust authentication methods more important than ever.

7. Other Considerations

Access arrangements and special requirements

- 7.1** All TLM's qualifications are intended to be accessible, as widely as possible.

Please refer to the Annex for further information.

Centres should contact TLM if they have any questions related to accessibility issues

Language

- 7.2** The language for provision of this qualification is English only. This will only change if we have a significant demand in another language that is sufficient to cover the additional costs involved.

Malpractice

- 7.3** TLM has comprehensive policies and procedures for dealing with malpractice. These are documented with links on the web site at <https://tlm.org.uk/policy-download-centre/>

Assessors should be familiar with these policies and make them clear to candidates. Assessors should inform their account manager if they suspect any instance of malpractice that could have a material effect on the outcome of any assessments, either for themselves or colleagues.

This is part of the upholding of standards that is part of the contract with TLM.

Equality of opportunity

- 7.4** TLM promotes equality of opportunity through policies and procedures. These are again documented in detail on the web site.

Resources, Support and Training

- 7.5** A clear goal is to enable learners to support all their IT user needs using resources freely and legally available from the internet. This is related directly to national policies for inclusion and equality of opportunity.

- 7.6** TLM does not require centres to use free and open-source software (FOSS), but it actively encourages its use, particularly in the context of embedded systems development and operations.

Most of the essential tools required to support the practical elements of these qualification, such as Linux distributions, code editors, compilers, network analysis tools, and system monitoring utilities, are freely available and widely used across industry.

By equipping learners with the skills and confidence to work with open-source technologies, we not only promote independence and digital resilience but also support the growing demand for professionals who can operate effectively in open, collaborative development environments.

The use of open-source resources also provides a cost-effective solution for schools, training providers, and learners, aligning with sustainable and inclusive approaches to digital education.

Annexe A

Level 2 Award in Cyber Security Awareness- Unit assessment - coursework guidance

The Level 2 learner reflects the ability to select and use relevant knowledge, ideas, skills and procedures to complete well-defined tasks and address straight-forward problems. It includes taking responsibility for completing tasks and procedures and exercising autonomy and judgment subject to overall direction or guidance. AND/OR Holder can select and use relevant cognitive and practical skills to complete well-defined, generally routine tasks and address straightforward problems. Holder can identify how effective actions have been. Holder can identify, gather and use relevant information to inform actions.

Moderation/verification: The assessor should keep a record of assessment judgements made for each candidate and make notes of any significant issues for any candidate. They must be prepared to enter into dialogue with their Account Manager and provide their assessment records to the Account Manager through the on-line mark book. They should be prepared to provide evidence as a basis for their judgements should it be required by the Principal Assessor or their Account Manager/external moderator. Before authorising certification, the Account Manager must be satisfied that the assessor's judgements are sound.

General Information

The Level 2 qualification has the following characteristics for learners:

- Achievement at RQF level 2 (EQF Level 3) reflects the ability to select and use relevant knowledge, ideas, skills and procedures to complete well-defined tasks. It includes.
 - Taking responsibility for completing tasks and procedures and exercising autonomy and judgement subject to overall direction or guidance.
 - Using understanding of facts, procedures and ideas to complete well-defined tasks and address straightforward problems.
 - Interpreting relevant information and ideas.
 - Taking responsibility for completing tasks and procedures subject to direction or guidance as needed.
-
- The specification for the Level 2 award provides an outcome framework for assessment and is not intended to dictate any particular context for learning and so can be used with any age range of adults

Requirements

- Standards must be confirmed by a trained Level 3 Assessor
- Assessors must as a minimum record assessment judgement as entries in the on-line mark book on the TLM certification site.
- It is expected that there will be routine evidence of work used for judging assessment outcomes in the candidates' records of their day-to-day work. Samples, including related plans and schemes of work should be available at the annual visit and/or by video conference.
- Different approaches to learning will be required in order to match differing needs, for example, the needs of learners will be different from the needs of those with learning disabilities.
- When the candidate demonstrates secure capability against each of the criteria in the unit, they are entitled to a certificate for passing the unit and the overall award.
- We expect at least 12 hours of guided study to be under-taken for the award for complete beginners generally new to formal education, but discretion can be used to take account of prior learning where this is sensible in individual cases. In terms of making the certificate, what matters is outcomes. Can the candidate securely meet the criteria?

MANDATORY UNIT

Level 2, Unit 1 – Cyber Security Awareness

1. Understand common cybersecurity threats, including social engineering, and their impacts	2. Understand how personal actions can expose organisational systems	3. Apply basic safe cyber practices in day-to-day work	4. Understand how to raise a suspected cyber incident promptly
1.1 Describe what is meant by a cyber threat	2.1 Identify two ways attackers manipulate staff to gain unauthorised access	3.1 Describe how to set up a strong password and enable multi-factor authentication.	4.1 Identify the correct internal route for reporting a suspected breach
1.2 List four common threats that exploit human behaviour	2.2 Identify a real-world incident where staff behaviour was exploited	3.2 Identify three warning signs of a phishing message	4.2 Describe the key information that should be recorded and passed on when reporting a breach
	2.3 Describe the impact on the organisation.		4.3 Describe why rapid reporting and preserving evidence are important

Teacher Guidance

1: Understand common cybersecurity threats, including social engineering, and their impacts

1.1 Describe what is meant by a cyber threat

- Introduce the idea of a *threat* as a potential cause of harm to systems, data, or services.
- Distinguish clearly between threats, vulnerabilities, and risk using plain, workplace-relevant examples (e.g., a convincing fake invoice is a *threat*; weak password practices are a *vulnerability*; the chance of payment being misdirected is the *risk*).
- Link to the confidentiality–integrity–availability (CIA) model to frame potential impacts without excessive technical detail.
- Encourage learners to use everyday language first, then apply correct terminology.

1.2 List four common threats that exploit human behaviour

- Explore the human factor through concrete social-engineering patterns: phishing and spear-phishing e-mails, vishing (phone), smishing (SMS), baiting/USB drops, tailgating/shoulder-surfing, and fake support calls.
- Use short case vignettes and screen captures to highlight *red flags* (mismatched URLs, urgent tone, authority pressure, unexpected attachments).
- Emphasise that attackers target habits and trust, not just technology.
- Ask learners to build a simple “threat and tell” glossary in their notes that names the threat and describes how it tries to make someone act.

1.3 Describe typical impacts on individuals and organisations

- Connect threats to operational disruption, financial loss, reputational damage, and legal/regulatory consequences.
- Encourage learners to think about short-term impacts (e.g., locked accounts, invoice delays) and longer-term effects (e.g., loss of customer trust, remediation costs).
- Use anonymised or public domain examples as discussion starters, keeping the focus on behaviours and consequences rather than specific brands.

2: Understand how personal actions can expose organisational systems

2.1 Identify two ways attackers manipulate staff to gain unauthorised access

- Teach core influence techniques: authority, urgency, scarcity/reward, and liking/reciprocity.
- Map each to typical workplace pretexts (e.g., “IT security here—your account will be disabled unless you confirm now”).
- Encourage learners to practise *challenge and check* methods (verifying via a known internal channel, not by replying or clicking links).
- Briefly introduce the idea of *least privilege* and why sharing credentials or propping doors open defeats organisational controls.

2.2 Identify a real-world incident where staff behaviour was exploited

- Guide learners to choose a credible case from reputable sources (press releases, regulator statements, independent reporting).
- The emphasis is on what the attacker did and which behaviours made it work—not on technical deep dives.

- Learners should summarise the incident in a few lines and note the human behaviours that were targeted (e.g., responding to urgency; trusting a spoofed sender).

2.3 Describe the impact on the organisation

- Extend the case by asking learners to describe one or two concrete impacts: service downtime, data exposure, customer notifications, internal investigations, or remediation costs.
- Encourage them to connect impacts back to the CIA model and to consider obligations that may arise under organisational policy or law (e.g., notifying the appropriate internal team; awareness of statutory timeframes where applicable), without requiring legal analysis.

3: Apply basic safe cyber practices in day-to-day work

3.1 Describe how to set up a strong password and enable multi-factor authentication

- Cover passphrases (e.g., three or more random words), uniqueness per account, the role of password managers, and secure storage of backup/MFA recovery codes.
- Walk through enabling multi-factor authentication (MFA) using typical factors (authenticator app, hardware key, or SMS where policy permits).
- Stress alignment to local organisational policy: what tools are approved, where to find instructions, and whom to contact if something goes wrong.
- If live configuration is not possible in class, use annotated screenshots or vendor demos to keep learning practical.

3.2 Identify three warning signs of a phishing message

- Analyse real but safe examples to spot display-name spoofing, mismatched links, unexpected attachments, grammar/branding anomalies, and pressure tactics.
- Reinforce the correct first action: do not reply, click, or forward outside the reporting route.
- Encourage learners to create a personal checklist they can apply at work (e.g., *pause—inspect—verify—report*).

4: Understand how to raise a suspected cyber incident promptly

4.1 Identify the correct internal route for reporting a suspected breach

- Show learners where the organisational policy lives and what the single point of contact is (service desk ticket, security mailbox, hotline).
- Discuss out-of-hours options and escalation if the primary route is unavailable.
- Emphasise that *reporting early is always better than trying to fix it alone*.

4.2 Describe the key information that should be recorded and passed on when reporting a breach

- Teach a simple reporting frame: who, what, when, where/how. Include: affected accounts/devices, relevant message headers or filenames, timestamps, and immediate steps already taken (if any).
- Encourage safe evidence handling (e.g., keep the e-mail in place; take a screenshot rather than forwarding suspicious content).

4.3 Describe why rapid reporting and preserving evidence are important

- Explain that quick, accurate reporting helps contain threats, protect other users, support investigation/forensics, and meet organisational and regulatory requirements.
- Reinforce that preserving evidence (logs, messages, device state) increases the chances of understanding the incident and preventing recurrence, while also supporting any formal notifications the organisation may need to make.

Accessibility Policy

TLM firmly believes that every learner should have an equal chance to excel in their studies and assessments, regardless of any disabilities they may have. To achieve this goal, TLM has developed a comprehensive and well-structured reasonable adjustment policy that is specifically tailored to cater to the needs of learners with disabilities. This policy is not only an essential aspect of TLM's commitment to inclusivity but also an integral part of creating a diverse and accessible learning environment.

The reasonable adjustment policy is designed to support learners with disabilities in various ways. It encompasses a range of accommodations, such as providing additional time for examinations, offering alternative formats for study materials, permitting the use of assistive technology, arranging for sign language interpreters, and ensuring accessible physical facilities. The implementation of these reasonable adjustments is meticulously carried out to ensure that they meet the individual needs of each learner, acknowledging the unique challenges they may face.

TLM is dedicated to making the reasonable adjustment process transparent and easily accessible for all stakeholders. Thus, the details of the policy are made readily available to all, including learners, educators, and TLM Centres. These details can be found on TLM's official website, ensuring that everyone is well-informed about the support and accommodations available to learners with disabilities.

Additionally, TLM Centres play a crucial role in facilitating this process. They are empowered to submit requests for other reasonable adjustments on behalf of learners, based on their specific requirements and circumstances.

TLM firmly believes that promoting a culture of inclusivity and understanding is fundamental to fostering an environment where learners can thrive, irrespective of their abilities or disabilities. By continuously evaluating and refining its reasonable adjustment policy, TLM ensures that it remains up-to-date with the best practices in the field of inclusive education.

TLM Qualifications is deeply committed to its duty as an awarding organisation to provide reasonable adjustments for learners with disabilities in accordance with the Equality Act 2010. By adhering to its comprehensive reasonable adjustment policy and collaborating closely with TLM Centres, TLM strives to create a learning landscape that supports and empowers all learners, ensuring they can reach their full potential and achieve academic success.

TLM Accessibility Policy: <https://tlm.org.uk/policies/general-requirements-for-regulated-qualifications/#3>

TLM reasonable adjustment policy: <https://tlm.org.uk/reasonable-adjustments-and-special-considerations-policy-2/>

TLM reasonable adjustments request form: <https://tlm.org.uk/wp-content/uploads/2022/03/TLM-RASC-form-1.docx>

Alignment with the CASLO Approach

This qualification has been designed in line with the principles of the CASLO approach, ensuring each unit is clearly defined in terms of learning outcomes and assessment criteria, with outcomes structured around observable knowledge, skills, and behaviours. In doing so, we embrace CASLO's strengths in transparency, clarity, and learner-centred planning for curriculum, teaching, and assessment.

While we recognise that CASLO qualifications are typically characterised by a mastery model, whereby all outcomes must be met to achieve a pass, we have chosen to adopt a holistic approach to evidence collection and assessment. This means learners may demonstrate their achievement of outcomes across multiple pieces of evidence, and assessors may consider a broader context of performance, rather than requiring separate, isolated confirmation for each criterion.

This approach supports:

- flexibility in delivery and learner pacing
- the integration of learning across units
- and better accommodates diverse learner journeys, particularly for adults returning to education or learners with mixed prior experience.

We are aware of the potential limitations of the CASLO model—such as the risk of learner failure due to narrowly missing a single outcome—and have mitigated this by embedding formative assessment opportunities and maintaining strong internal quality assurance to support valid, reliable, and fair judgements.

By doing so, this qualification respects the CASLO model's intent—to confirm specified learning outcomes—while avoiding overly rigid application of the mastery principle that could undermine learner success or the demonstration of real-world competence.