Cyber Security Awareness Training Service Definition

Document title	Cyber Security Awareness Training Service Definition		
Reference No.	IF-SER-030	**Version**	0.1 Draft
Author	Holly Jackson, Cyber Manager		
Reviewed by	Lisa Washer, Head of Cyber		
Issue date	26/01/2026		

Cyber Security Awareness Training Service Definition

Document Control

Version	Name	Comment	Date
0.1	Holly Jackson	Initial draft	07/01/2026
0.2	Lisa Washer	Review and amendments	25/01/2026
1.0	Holly Jackson	Final review and publish	26/01/2026

Correlation Chart

Clause	FSR Code of Practice v2	ISO/IEC 17025:2017	ILAC-G19 :06/2022	ISO 9001:2015	ISO/IEC 27001:2022
Review of Requests, Tenders and Contracts	16	7.1	4.1, 4.7	8	4.2

Contents

1. Cyber Security Awareness Training

1.1 Service Overview

1.1.1 The Cyber Security Awareness Training service is designed to improve organisational resilience by enhancing staff knowledge, behaviours, and decision-making related to cyber security threats. The service delivers interactive, engaging training sessions tailored to the client's environment, industry sector, and risk profile.

1.1.2 The training equips employees with the practical skills required to identify and respond to common cyber threats such as phishing, social engineering, password compromise, data handling risks, and emerging cyber-attack methods. The purpose is to reduce human-related security incidents and foster a culture of cyber awareness across the organisation.

2. Service Features

2.1 Core Features

2.1.1 The following outlines the core features of the training service:

a) **Customised Training Materials -** Training content is tailored to the client's operational environment, industry risks, policies, and maturity level. Modules are developed to align with the organisation's cyber strategy and regulatory requirements.

b) **Live Instructor-Led Training Sessions -** In-person or virtual training sessions delivered by certified cyber security professionals. Sessions include real-world examples and interactive Q&A.

c) **Role-Based Training Packages -** Specialised training delivered either remotely or on site to focus on the unique risks associated with roles such as finance, HR, IT administrators, executives, and customer-facing teams.

d) **Executive & Leadership Briefings -** Dedicated strategic briefings for senior leadership teams, delivered either remotely or in person. These sessions address current threats, governance responsibilities, and decision-making considerations during cyber incidents.

e) **Annual Review of Training Programme -** A yearly review of training effectiveness, content updates, lessons learned, and alignment with new threats and organisational changes.

3. Service Benefits

3.1.1 The following lists the key outcomes and advantages the customer gains from using the service.

a) **Reduced Cyber Risk Exposure -** Employees make safer decisions, reducing successful phishing, malware, and social engineering attacks.

b) **Improved Compliance -** Supports adherence to regulatory requirements such as GDPR, PCI DSS, ISO 27001, and internal policies.

c) **Strengthened Security Culture -** Encourages ongoing awareness and shared responsibility for security across all departments.

d) **Measurable Performance Tracking -** Data-driven insights into staff behaviour, high-risk areas, and training impact.

e) **Customisable Delivery -** Flexible options to suit different teams, schedules, and learning styles.

4. Scope of Service

4.1 In-scope activities

4.1.1 The scope of the service includes the following activities:

a) Delivery of live instructor-led training

b) Development of client-specific training content

c) Execution of phishing simulations

d) Reporting on training and simulation performance

e) Advisory on awareness strategy and behavioural improvement

4.2 Out-of-scope activities

4.2.1 The following activities are not included as part of the service scope. However, the organisation can provide support for these activities through additional services or established partner arrangements, subject to separate agreement:

a) Enforcement of staff compliance or internal HR actions

b) Development of full cyber policies outside training content

c) Remediation of cyber incidents

d) Custom learning platform development unless explicitly agreed

4.3 Assumptions and dependencies

4.3.1 Delivery of the service is subject to the following assumptions, constraints, and dependencies, which influence scope, timelines, and outcomes.

a) Client provides necessary staff attendance and communication

b) Access to internal policies or risk areas to tailor training

c) Ability to send simulated phishing emails to staff (technical approvals required)

5. Onboarding

5.1.1 Onboarding begins with a discovery session to understand the client's environment, objectives, staffing profiles, and regulatory requirements. This is followed by the development of a customised training plan, preparation of phishing simulation schedules, and confirmation of reporting formats. All stakeholders, escalation paths, and communication channels are documented prior to service commencement.

6. Service Delivery Model

6.1.1 The service is delivered through a structured combination of live instructor-led training sessions, ongoing behavioural reinforcement, and periodic assessment activities. This blended approach ensures that staff not only receive foundational cyber security knowledge but also continue to develop secure behaviours over time. The model focuses on sustained learning, practical understanding, and measurable risk reduction.

6.2 Planning & Design

6.2.1 This initial phase involves detailed requirements gathering to understand the client's organisational structure, risk profile, operational environment, and training objectives. During this stage, the training calendar is designed in collaboration with the client, ensuring sessions are scheduled in alignment with business needs and availability. Training materials are customised to reflect the client's internal policies, industry-specific threats, and preferred delivery format—whether remote, on site, or a combination of both.

6.3 Training Delivery

6.3.1 Training is delivered through live instructor-led sessions, either conducted remotely via secure video conferencing or delivered on site at client premises. These sessions are interactive and practical, incorporating real-world scenarios, discussions, and opportunities for participants to ask questions.

6.4 Reinforcement Activities

6.4.1 To support retention of knowledge and encourage continuous behavioural improvement, reinforcement activities such as phishing simulations and short refresher engagements are conducted throughout the year. These activities help assess how effectively staff are applying their learning in real-world scenarios and highlight areas where further support or targeted training may be required.

6.5 Reporting & Review

6.5.1 Following each training cycle or reinforcement activity, detailed reporting is provided. This includes analytics on attendance, participation, phishing simulation outcomes, and identified behavioural trends. Periodic review sessions are held with key stakeholders to discuss performance, measure progress against training objectives, and agree on any adjustments or future enhancements to the programme.

6.5.2 The entire service is flexible and can be delivered remotely, on site, or through a hybrid model depending on client preference, geographical distribution, and operational requirements. This ensures the training programme can be adapted to a wide range of organisational structures and working arrangements. Training sessions can also be provided on an adhoc basis.

7. Support Model

7.1.1 The service includes business hours support, available Monday to Friday from 09:00 to 17:00, to assist with any training-related queries or operational questions. Any issues that require further attention follow a defined escalation path, progressing from the Training Coordinator to the Service Manager, and ultimately to the Head of Cyber if necessary. For clients requiring additional flexibility, optional support enhancements are available, including extended support hours, additional phishing simulations, and bespoke training content tailored to specific organisational needs.

8. Service Level Agreements

8.1.1 The following service levels describe indicative performance targets for the service. These service levels are provided for guidance only and do not constitute guaranteed commitments unless expressly agreed in writing.

8.2 Response time

8.2.1 All email enquiries will be responded to within one business day, ensuring timely communication and support. Any issues requiring escalation will be raised to the appropriate service level within four working hours to minimise disruption and maintain service continuity.

8.3 Delivery timeframe

8.3.1 The training delivery schedule will be confirmed during onboarding, tailored to the client's availability and operational needs. Where customised materials are required, these will be produced within 10–20 business days, depending on the complexity and depth of customisation requested.

8.4 Reporting turnaround

8.4.1 Training reports will be provided within five business days following the completion of each session, offering a summary of attendance and key observations. Reports for phishing simulations will be issued within three business days, ensuring timely insight into staff behaviours and risk areas.

9. Technical Requirements

9.1.1 The following requirements apply and are confirmed during onboarding.

a) **Video/web conferencing tools for virtual sessions** - The client must provide access to approved video or web-conferencing platforms to enable the delivery of remote instructor-led training sessions. These tools should support screen sharing, audio and video communication, and interactive features such as chat or polling to ensure effective participant engagement. Platforms may include Microsoft Teams, Zoom, or similar solutions, depending on the client's internal policies and security requirements.

b) **Ability to run phishing simulation emails through client mail systems** - To conduct phishing simulations effectively, the client's email infrastructure must allow authorised simulation emails to be delivered to user inboxes. This may require adjustments to security filters, whitelisting trusted domains, or temporarily modifying email gateway rules.

c) **User availability** - Employees must be made available to attend scheduled training sessions, whether remote or on-site, to ensure the success of the awareness programme. Adequate time should be allocated within working hours to allow participants to fully engage with training activities, simulations, or reinforcement exercises without operational disruption.

d) **Company and environment information to tail training to objectives** - The client is expected to provide relevant information about their organisation, such as internal policies, key risk areas, technologies used, and existing security challenges. This information is used to tailor training content, examples, and scenarios so that sessions align with the organisation's objectives, industry risks, and operational realities.

10. Exit and Offboarding

10.1.1 Upon conclusion of the service, the provider will deliver all final outputs to the client, including reports, performance analytics, training materials, and any additional documentation generated throughout the engagement. These deliverables ensure the client has full visibility of the activities undertaken, the outcomes achieved, and any recommendations for ongoing improvement. Following the transfer of materials, any client data that was accessed, stored, or generated as part of the service will be securely deleted or returned in accordance with contractual obligations and agreed data-handling procedures. This includes adherence to relevant security controls, retention policies, and industry best practices to ensure the confidentiality and integrity of client information.

11. Roles and Responsibilities

11.1.1 The following roles are defined to ensure effective delivery of the service:

11.2 Provider Responsibilities

11.2.1 The provider is responsible for delivering all scheduled training sessions and phishing simulations as part of the agreed programme. They will produce the required reports and analytics that summarise participation, performance, and behavioural trends, ensuring the client has clear visibility of outcomes. The provider will also maintain up-to-date training materials that reflect current threats, best practices, and organisational needs. In addition, the provider is accountable for ensuring that all trainers and support staff involved in delivering the service are appropriately qualified, competent, and equipped to deliver high-quality, effective cyber security awareness training.

11.3 Client Responsibilities

11.3.1 The client is responsible for coordinating staff attendance to ensure that all relevant employees are available for scheduled training sessions and simulations. They must also provide the information required to tailor the programme effectively, including organisational details, policies, and key contacts. In addition, the client is expected to review and approve all planned phishing simulation exercises before deployment, ensuring they align with internal expectations and governance requirements. Finally, the client should support the internal communication of the training programme, helping to promote awareness, encourage participation, and reinforce the importance of cyber security across the organisation.

*****END OF DOCUMENT*****