



G-Cloud 15 Service Definition Document

Security Education Training & Awareness

Executive Summary

Our Security Education Training & Awareness (SETA) service empowers employees to become an active line of defence against cyber threats. By combining targeted training, continuous awareness activities, and measurable outcomes, we help organisations reduce human-related security risks and strengthen their overall security posture.

The service delivers role-based security training and ongoing awareness initiatives designed to improve employees' understanding of cybersecurity risks, policies, and best practices. The program focuses on practical, real-world scenarios to ensure knowledge is retained and applied in day-to-day activities.

About Inductive Solutions

We are a specialist consultancy delivering Cyber Security, Red Teaming, Cloud FinOps, and Predictive Intelligence. Founded by a veteran, we bring a disciplined approach to complex government challenges.

Our team is built on three core pillars:

1. **Strategic Command:** We apply proven leadership principles to bring order to complex programmes.
2. **Cybersecurity:** We integrate security into the foundation of every service, not as an afterthought.
3. **Data Science & Insight:** We model outcomes using data and facts, providing certainty in decision making.

Social Value & Corporate Responsibility

We are committed to delivering value beyond the contract:

- **Veteran founded:** We bring the ethos of service and discipline to our engagements.
- **Disability Confident:** We are committed to recruiting diverse talent to ensure we have varied perspectives required to solve complex challenges.



- **Armed Forces Covenant Pledge:** We are in the process of submitting our Armed Forces Covenant Pledge to formalise our support to the Armed Forces community.
- **Women in STEM:** We actively promote gender diversity to close the skills gap in technical roles.
- **Net Zero:** We are on track to achieve Net Zero by 2030 through sustainable business architecture and remote-first working practices.

Service Overview

Our SETA service delivers role-based security training and ongoing awareness initiatives designed to improve employees' understanding of cybersecurity risks, policies, and best practices. The program focuses on practical, real-world scenarios to ensure knowledge is retained and applied in day-to-day activities. The SETA service can be delivered through a combination of online training, live workshops, simulated exercises, and continuous awareness materials, tailored to the organisation's size, industry, and risk profile.

Features and Benefits

Service Features

- **Security Awareness Training:** Interactive training sessions covering topics such as phishing, password hygiene, data protection, remote work security, and incident reporting.
- **Role-Based Education:** Customised training for different roles (e.g., general users, executives, IT staff) to address specific risks and responsibilities.
- **Phishing & Social Engineering Awareness:** Simulated phishing campaigns and targeted education to improve detection and reporting of suspicious communications.
- **Ongoing Awareness Campaigns:** Regular awareness activities including newsletters, micro-learning content, posters, and security tips to reinforce key messages throughout the year.
- **Policy & Compliance Alignment:** Training aligned with internal security policies and relevant standards or regulations (e.g., ISO 27001, NIST, GDPR).
- **Measurement & Reporting:** Metrics and reports to track participation, effectiveness, and improvement over time, supporting audit and compliance needs.

Service Benefits

- **Reduced Likelihood of Cyberattacks:** Reduces the likelihood of successful cyberattacks by identifying threats early.



- **Improved Employee Confidence:** Improves employee confidence in identifying and responding to threats.
- **Stronger Compliance:** Ensures stronger compliance with security standards and regulatory requirements.
- **Measurable Improvement:** Delivers a measurable improvement in organisational security culture.
- **Risk Reduction:** Reduces the risk of security incidents caused by human error.
- **Increased Awareness:** Increases awareness of cyber threats such as phishing, social engineering, and malware.
- **Secure Behaviours:** Promotes secure behaviours aligned with organisational policies and regulatory requirements.
- **Security Culture:** Builds a strong, organisation-wide security culture.

Our Methodology

The SETA service is delivered through a structured combination of training methods tailored to the organisation's size, industry, and risk profile.

Targeted Training & Workshops

We provide interactive training sessions covering topics such as phishing, password hygiene, data protection, remote work security, and incident reporting. This includes customised training for different roles (e.g., general users, executives, IT staff) to address specific risks and responsibilities.

Simulated Exercises

We utilise simulated phishing campaigns and targeted education to improve the detection and reporting of suspicious communications.

Continuous Awareness & Measurement

We deliver regular awareness activities including newsletters, micro-learning content, posters, and security tips to reinforce key messages throughout the year. We provide metrics and reports to track participation, effectiveness, and improvement over time, supporting audit and compliance needs.

Onboarding and Offboarding

Pre-boarding Process

To ensure compliance from the start of the engagement we follow a standard pre-boarding protocol in preparation for project delivery.

1. **Compliance & Contracting:** Exchange of Contracts, NDAs, and Statements of Work via secure digital signing to prevent administrative delays.



2. **Security Vetting:** Pre-submission of all consultant details to the Client Security Controller to ensure site and network access upon start of project.
3. **Technical Access:** We provide a prerequisite list of technical access requirements to allow the client to issue IT permissions.

Onboarding Process

Our Onboarding process is designed to ensure our team is operational and delivers value from Week 1, without administrative delays:

1. **Success Criteria & Scope:** A formal workshop to introduce the team, define specific outcomes, Key Performance Indicators (KPIs), and boundaries of the project.
2. **Communication Schedule:** We establish a clear routine for updates, agreeing on the exact format and timing of reports to ensure transparency.
3. **Stakeholder Mapping:** We identify key decision-makers and subject matter experts required for interviews and data gathering.
4. **Evidence Gathering:** We move immediately into discovery and access logs, billing data, or legacy documentation to establish a factual baseline.
5. **Early Value Delivery:** We aim to deliver an initial findings report within the first few weeks (if applicable to the project scope).

Offboarding & Knowledge Transfer

We plan for offboarding from the start of the engagement. Our goal is to leave the client capable of managing the service independently, ensuring sustainable long-term value.

1. **Knowledge Transfer:** We conduct structured handover sessions with permanent staff to explain strategies, operational processes, or maintenance requirements. We focus on upskilling your internal teams to ensure operational independence.
2. **Documentation & Deliverables:** We provide a full handover of all contractually agreed outputs.
3. **Intellectual Property:** While the Client owns the specific deliverables created for them and specified in the contract, Inductive Solutions retains ownership of its methodologies, models and all other Intellectual Property. We do not transfer our proprietary internal tools or code libraries unless explicitly agreed to in the contract prior to the start of the engagement.
4. **Secure Data Deletion & Asset Return:** Upon project closure, we execute a secure data destruction process. Client data is permanently deleted from our systems in compliance with GDPR and government security standards, with a confirmation certificate provided if required. Any assets belonging to the client are dutifully returned.
5. **Closure Report:** We submit a final engagement report summarising the outcomes achieved, lessons learned, and recommended next steps.



Service Constraints & Requirements

- **Scope:** All services are subject to scope.
- **Role-based education:** Dependency on role definitions.
- **Simulated phishing:** Campaigns and targeted education are required.
- **Awareness Campaigns:** Ongoing campaigns are part of the service restriction.
- **Alignment:** Policy & Compliance Alignment is required.
- **Reporting:** Metrics and reports to track participation, effectiveness, and improvement are subject to data availability.

Service Levels & Support

- **Account Management:** An Account Manager is available for escalations.

Standard Support Hours

Our standard support hours are 9:00 - 17:00 GMT/BST, Monday to Friday (excluding UK Public Holidays).

Support is available via:

- **Email:** For general enquiries, reporting, and non-urgent issues.
- **Phone:** For urgent matters and immediate escalation.

Account Management

Every engagement is assigned a dedicated Programme Delivery Manager to ensure quality and alignment with strategic goals. Clients also have a direct escalation route to the Company Directors if required.

Security & Business Continuity

Security Vetting & Personnel

- **Clearance:** All consultants hold a minimum of BPSS (Baseline Personnel Security Standard) clearance. We can submit staff for SC (Security Check) and DV (Developed Vetting) clearances for sensitive engagements upon request, if sponsorship is provided by the Client.
- **Training:** All staff undergo regular security awareness training and data handling instruction.

Data Security and Encryption

- **Data Residency:** Client data is processed and stored within the United Kingdom and the European Union (EU), in full compliance with UK GDPR and the Data Protection Act 2018.



- **Data Sovereignty:** Strict Data Sovereignty (guaranteed processing and storage solely within the UK) is available upon request, subject to a minimum contract size.
- **Encryption:** We enforce strict encryption policy. All data is encrypted in transit and at rest to ensure confidentiality and integrity.
- **Secure Communication:** Standard email communication is secured via TLS. Enhanced End-to-End Encryption is available upon request, subject to a minimum contract size.
- **Accreditation:** We are Cyber Essentials certified, demonstrating our commitment to fundamental cybersecurity controls.

Business Continuity & Resilience

- **Cloud Native Model:** We operate a secure, cloud-native business model. We do not rely on physical on-premise servers or single-site infrastructure. This ensures that our services are resilient to physical site failures.
- **Remote Working:** Our systems and security architecture support secure remote working. In the event of a physical office disruption, our team can continue to deliver services remotely without operational downtime.
- **Backup & Recovery:** All critical business data is backed up securely in the cloud with redundancy to ensure data availability and rapid recovery.

Pricing

Pricing is directly linked to the Project Scope and complexity of the requirement.

- We work with the Client to define the specific deliverables and timeline.
- We estimate the resource effort required to deliver that scope.
- We apply the corresponding daily rates from our SFIA Rate Card to calculate the total engagement cost.

All daily rates are listed in our separate SFIA Rate Card (Skills Framework for the Information Age). Our daily rates are fully inclusive of all consultant overheads, equipment, software tools (except client systems), and insurance. We do not charge administrative fees.

Discounts

To deliver maximum value to the public sector, we offer the following discounts:

- **Educational Discount:** We offer a standard discount to schools, colleges, and universities (institutions with [.ac.uk](https://www.ac.uk) domains).
- **Volume Discounts:** Volume discounts are available for long-term engagements or large team deployments. These are applied on a sliding scale based on the total number of days purchased.