



G-Cloud 15 Service Definition Document

Audit and Assurance

Executive Summary

Audit and Assurance is a comprehensive compliance service designed to help Government departments and supply chain partners achieve and maintain critical security standards, including Cyber Essentials (Plus), IASME Cyber Assurance, ISO27001, and ISO42001 (Artificial Intelligence Management System).

We combine strategic discipline, cybersecurity expertise, and advanced data science to deliver outcomes that are operationally executable. We use gap analysis and remediation support to build genuine cyber resilience. Whether preparing for an external surveillance audit or seeking first-time certification, we ensure your organisation achieves robust security, compliance, and continual improvement.

This service is designed for Senior Responsible Owners (SROs), CISOs, and Programme Directors who require robust, secure, and data-driven delivery.

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

Comprehensive cybersecurity services tailored to UK and International Standards, including gap analysis, advisory, verification, audit, and certification across Cyber Essentials (Plus) and IASME Cyber Assurance. We also provide readiness support for ISO 27001 and ISO/IEC 42001 (AI Management System). We ensure organisations achieve robust security, compliance and resilience through tailored expert support programmes.

Features and Benefits

Service Features

- **Cyber Essentials:** Gap Analysis, Advisory, Verification, and Certification.
- **Cyber Essentials Plus:** Technical Audit, Vulnerability Scanning, and Certification.
- **IASME Cyber Assurance:** Level 1 (Verified Assessment) and Level 2 (Audit) Certification.
- **ISO 27001:** Gap Analysis, ISMS Design, and Surveillance Audit Readiness.
- **ISO/IEC 42001:** Artificial Intelligence Management System (AIMS) Design & Risk Assessment.
- **Cyber Baseline:** Level 1 Verification and Certification.
- **Remediation Support:** Practical, hands-on advice to fix identified non-compliances.
- **AI Risk Management:** Alignment with NIST AI RMF and ISO 42001 principles.

Service Benefits

- **Reduces Business Risk:** Lowers compliance costs through structured certification readiness.
- **Streamlines Workflows:** Aligns security controls with daily operations to minimise friction.



- **Accelerates Certification:** Removes inefficiencies and "guesswork" from the audit process.
- **Enhances Decision Making:** Provides clear visibility of security maturity and risk exposure.
- **Supply Chain Confidence:** Demonstrates to partners and Government buyers that data is protected.
- **Operational Efficiency:** Embeds security into the lifecycle rather than treating it as an afterthought.
- **Right-First-Time:** Minimises rework by ensuring compliance documentation is accurate from the start.
- **Expert Access:** Direct access to IASME-licensed Assessors and GRC specialists.

Our Methodology

We approach every engagement with a structured, three-phase methodology.

Phase 1: Evidence-Based Discovery & Baseline:

We begin by establishing the facts. Whether for Cyber Essentials or ISO standards, we conduct a Gap Analysis against the relevant framework.

- **For Cyber Essentials:** We review your answers and technical controls (firewalls, patching, access control) to identify immediate failures.
- **For ISO Standards:** We audit your existing policies and procedures against the clauses of the standard to produce a detailed "Readiness Report".

Phase 2: Strategic Architecture & Design:

Using the evidence from Phase 1, we help you close the gaps by providing pragmatic remediation advice.

- **Technical Fixes:** We assist your IT teams in understanding specific requirements.
- **Policy Design:** We draft or refine the required governance documentation.
- **Pre-Audit Validation:** We conduct pre-assessments to ensure you are ready for the formal certification body.

Phase 3: Delivery & Sustainment:

We move to the formal assessment phase with confidence.

- **Verification:** we verify your self-assessment or conduct the technical audit (for CE Plus/Cyber Assurance Level 2).
- **Certification:** Upon successful completion, we issue the relevant certificates and logos.
- **Sustainment:** For ISO standards, we prepare you for the External Surveillance Audit, ensuring you maintain compliance over the 3-year cycle.



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 Dependent:** Timescales vary based on organisation size, complexity, and current maturity.
- **No Guarantee of Pass:** Completion of an assessment does not guarantee certification; non-compliances must be fixed.
- **Remediation Delays:** significant gaps may exist between the start and completion of an assessment if the client takes time to remediate issues.
- **CE Plus Stages:** Cyber Essentials Plus is a multi-stage audit requiring vulnerability scanning; technical failures will result in a fail until fixed.
- **Client Resources:** Successful delivery requires access to technical stakeholders and permission to scan/audit systems.

Service Levels & Support

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](#) 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.