PEN TEST PARTNERS

G-Cloud 15

Lot 3 Cloud Support – Security Services Definition Document – GRC Consultancy

Version 1.0

Contact: bidteam@pentestpartners.com

Table of Contents

Your Trusted Partner

Penetration Testing

- Regulated CHECK Testing
- Infrastructure Testing
- Web, API & Mobile App Testing
- Compiled App Testing
- Application Code Reviews
- Cloud Threat Actor Simulation
- DevOps & CI/CD
- Kubernetes & Containerisation

Bespoke Services

- Regulated Red Teaming (CBEST, GBEST, STAR-FS, TIBER)
- Purple Teaming
- Cyber & Physical Social Engineering
- OT & ICS Security Testing
- Attack Surface Management / Assessment
- IoT, IIoT & Hardware Testing
- Aerospace & Satellite
- Maritime, Rail & Automotive Cyber Security

Digital Forensics & Incident Response

- Incident Response (email compromise, data exfiltration & recovery, e-discovery, root cause & impact)
- Digital Forensics & Expert Witness
- IR Maturity Assessment
- Compromise Assessments
- First Responder Training
- Ransomware Assessments
- Identity Risk Assessments

GRC Consultancy

- Architecture & Secure Design
- Cloud Review & Support
- Gap Analysis & Maturity Assessment
- PCI Consultancy (SAQ Support & ASV Scanning)
- vCISO Services
- Business Continuity Planning & Disaster Recovery
- Tabletop Exercise & Simulation
- ISO27001 Gap Analysis & Implementation
- Cyber Essentials (Plus)
- CAA Assure / Gov Assure
- Vulnerability Management
- Security Awareness

About Us

Pen Test Partners (PTP) has been providing cyber security expertise to a huge variety of industries and businesses since 2010. We are the largest independent security testing and consultancy business in the UK with over 150 employees across the UK and US. PTP tests the security of all computer and internet connected devices, applications, software, hardware, operational technologies (OT / ICS) & cloud services. The security testing team is supported by experienced consultants specialising in ISO 27001, PCI, Cyber Essentials and vCISO amongst others. The PTP offering is completed by an NCSC CIR Standard Digital Forensic Incident response (DFIR) capability.

As one of the founding members of the CREST scheme in the UK and US and as a previous CVE board member, we have helped to shape cyber security standards and frameworks like CBEST. Through our CBEST accreditation we are regulated by the Bank of England (BoE) and Prudential Regulatory Authority (PRA) and through our CHECK accreditation we are closely aligned to the National Cyber Security Centre (NCSC) Framework.

We are one of just a few providers accredited with the coveted CBEST UK Threat Intelligence Led Penetration Testing standard which allows us to test on behalf of British Government (GBEST/GCASE) and the Bank of England/FCA (CBEST/STAR). We are also approved by the Civil Aviation Authority to provide ASSURE services.

Our applicable certificates to deliver our clients with best-in class cyber security services include CHECK, CREST, CBEST, STAR, TIBER, PCI QSA, Cyber Essentials Plus, ASSURE and NCSC CIR Standard. We are also ISO 27001 certified across our entire business operations.

Service Definition Overview

PTP delivers specialist Governance, Risk & Compliance (GRC) services, supporting organisations across all sectors—including government, defence, critical national infrastructure, healthcare, finance, and commercial enterprises. Our services help organisations build resilient governance structures, strengthen security controls, and meet the regulatory, contractual, and assurance requirements essential for operating securely in complex digital environments.

Why PTP

- Deep expertise across defence, critical national infrastructure, finance, and enterprise
- Combination of strategic governance understanding and hands-on technical knowledge
- Independent, transparent, and aligned to recognised industry standards
- Proven ability to simplify complex requirements into practical, manageable actions
- Flexible engagement models including project-based, retainer, or vCISO support

PTP GRC Services:

- Cloud Services
  M365 Review
  M365 Enhancement
- Cyber Security Maturity Assessment
- Security Policy Review & Alignment
- vCISO (Virtual Chief Information Security Officer) and Support Service
- Cyber Essentials & Cyber Essentials Plus
- PCI DSS Services (can also be a Managed Service)
- ISO 27001 Services (can also be a Managed Service)
- UK Defence Cyber Certification (DCC)
- ISO 42001 Compliance

PTPs Approach to Working Together and Pricing

Every project we deliver is custom managed. From initial scoping through to debrief we will ensure the right approach and people are being utilised.

PTP's implementation plan typically follows an established workflow based on actions from PTP and our clients, although we can of course work around a client if they have a preferential implementation model.

PTP typical working model:

- **Dedicated Account Manager:**
  - PTP will allocate a dedicated account manager as a central point of contact for the duration of the relationship.
- **Initial Consultation:**
  - For each new engagement, PTP will initiate a conversation via email and/or call to understand your service requirements. This serves as the introduction call.
- **Scope of Works (SOW) Creation:**
  - A PTP technical consultant will review all relevant information and create a detailed Scope of Works (SOW). This document will include any necessary prerequisites.
- **Proposal and SOW Delivery:**
  - PTP will send a comprehensive Proposal/SOW, specifying:
    - Duration
    - Cost
    - Grade of consultant required
    - Proposed dates (if already discussed)
- **Pricing Calculation:**
  - Pricing will be determined based on the number of days required to deliver the services using the service day rates.
- **Acceptance of Proposal / SOW**
  - Upon acceptance of the SOW, delivery dates are agreed and scheduled.
- **Authorisation and pre-requisite information**
  - PTP will send a Authorisation form for signature and return.
- **Pre engagement Kick off Call**
  - PTP will host a pre-engagement call to discuss the engagement and introduce the team.
- **PTP undertakes the required services.**

PTP GRC Services Lines

Cloud Services - M365 Review / M365 Enhancement

Focusses on optimising Microsoft 365 environments through comprehensive reviews and enhancements. PTP help organisations maximise productivity, security, and compliance by identifying configuration gaps, implementing best practices, and tailoring solutions to business needs.

M365 Review

This service offers a point-in-time review of a client's Microsoft 365 tenant based on the latest guidance from Microsoft and the Centre for Internet Security (CIS) as well as general security best practices. The purpose of this review is to identify misconfigurations, insecure default settings and other security issues before they can be exploited by threat actors.

Several domains are covered during our Microsoft 365 Review, these domains focus on key areas such as identify and access management, application permissions, data management, email security, auditing, storage, and mobile device management. The process consists of a manual audit of the Microsoft 365 administration portals, completion of PowerShell commands, and a review of the client's processes and procedures in relation to Microsoft 365. The client will be provided with a comprehensive report that details the findings and outlines recommendations that can be used to further improve the security posture of their Microsoft 365 tenant.

Scope

To establish the current security controls, a review is required that will include:

- Control of administrative access of the M365 platform, by technical team including Multi-Factor Authentication (MFA) and conditional access configuration.
- Current processes for onboarding and offboarding users into the M365 environment.
- Security and Policy configuration within the individual M365 product offerings.
- Alerting configuration to produce actionable intelligence for follow up and incident response.
- SharePoint and OneDrive configuration best practice review based on CIS Foundation Benchmark and issues PTP typically experiences.

Whilst the M365 platform provides a level of security controls and default policy, consideration should also be given to the interface with the technical team.

A review of any processes relating to general IT administration or specific processes for M365 will also be included, through a short interview with staff.

Approach

PTP - To conduct the review, the following approach will be taken:

- Access to M365 admin dashboard as Global Reader is required. The majority of the review will be conducted without requiring client involvement.
- A remote interview with the technical team. This interview is conducted on day 3 or 4 of the engagement to confirm:
  - Services currently in use
  - Planned new services as M365 is adopted

- Current processes such as onboarding and offboarding of staff access, alert management and use of reporting or SIEM integration to identify issues

Costs provided are based on the availability of remote access and teams interview sessions being available. Local review requirements will incur additional expenses to attend site, and work with technical teams in the office location.

Client - In order to complete the review process, PTP will require the following access permission:

- Provide PTP with access to an M365 guest user, that is a member of the client domain and is assigned the 'Global Reader' role in the M365 admin portal

- Please avoid using SSO and accounts linked to @pentestpartners.com, as this doesn't allow switching between tenants correctly and prevents access to the required admin portals.

- Run a set of PowerShell commands to provide additional information for the report, based on a template provided by PTP.

PTP require that the client performs any remote PowerShell commands as significant changes and permissions are needed to allow PTP to run these on the client's behalf. The commands that need to be run should take no more than 10-15 minutes to produce the required output. This can be provided as screenshots as during a screen sharing session as required.

If this step cannot be completed, it will lead to the production of a partial report as currently the settings are not exposed in the standard web administration portals. PTP are constantly reviewing this situation and will ensure any client interaction is kept to a minimum.

M365 Enhancement

This is a service where PTP will work with the client to identify, plan, and implement security controls within the configuration of the client's Microsoft 365 tenant to further improve the organisation's security posture. Following the completion of a Microsoft 365 Review, PTP shall aid the client in implementing the recommended security controls. We can make the necessary configuration changes on behalf of the client or guide the client through the implementation of changes.

Phase 1 - Baseline security and license review

If a review of a client's Microsoft 365 tenant has not already been undertaken, this phase will consist of a brief review of the license set and the tenant configuration. Although some configuration changes may have already been implemented, there remains a possibility that some default settings are still in place. The output of this review shall be a baseline snapshot of the existing posture. This shall determine which controls need to be implemented during the remaining phases.

This will also provide PTP and the client with an understanding of which security features and functionality can be implemented under the existing license set. It is estimated that this will require one day to complete.

For Phase 1 to be undertaken successfully, a client must provide PTP with an internal account in their Microsoft 365 tenant. A guest account cannot be used. The internal account allocated to PTP must be assigned the 'Global Reader' role within Microsoft Entra ID (formerly Azure AD).

Phase 2 - M365 enhancement and remediation work
The focus of Phase 2 shall be to implement the desired functionality and any additional enhancements that were identified during the Phase 1 review along with all the requirements defined within the Engagement Scope.

To prevent disruption to a client's users and business operations, PTP would request to be supplied with a clients mobile device and a workstation (virtual machine is an option) that are registered with Entra ID and enrolled in Microsoft Intune. PTP would also recommend designating a group of pilot users who would be willing to have their user accounts and devices enrolled in new features.

This will allow the client and PTP to test the implementation of new functionality and security controls before they are deployed to the wider business.

For Phase 2 to be undertaken successfully, the client must provide PTP with an internal account in their Microsoft 365 tenant. This account must be assigned the 'Global Admin' role within Microsoft Entra ID. This account must not be a tenant guest user.

In addition to making direct configuration changes within the client's Microsoft 365 tenant, PTP can also support the client to undertake any configuration themselves. Therefore, a series of knowledge sharing sessions or workshops may also be applicable.

As there is a requirement for flexibility, the implementation shall be planned and coordinated between Pen Test Partners and the client on a call-off basis.

Cyber Security Maturity Assessment

PTP deliver Cyber Security Maturity Assessments to evaluate your organisation's security posture against industry standards. This service provides actionable insights to strengthen defences, reduce risk exposure, and align with regulatory requirements.

Key Features include:

- Assessment of the organisation's current cyber security maturity
- Benchmarking against recognised frameworks (e.g. NIST CSF, ISO/IEC 27001)
- Review of security governance, policies, and operating model
- Risk management and threat identification capability assessment
- Identity and access management maturity review
- Incident response, detection, and recovery capability review
- Vulnerability management and patching process assessment
- Third party and supplier security maturity review
- Identification of strengths, gaps, and control weaknesses
- Risk based prioritisation of improvement areas
- Executive level findings mapped to business impact
- Current state vs target state maturity comparison
- Pragmatic recommendations aligned to organisational risk appetite
- 12–24 month cyber security improvement roadmap

Security Policy Review & Alignment

PTPs policy review service ensures your security and compliance policies are up-to-date, aligned with frameworks such as ISO and NIST, and tailored to your operational environment. This helps maintain governance and regulatory compliance.

Key Features include:

- Catalogue all current security policies, standards, guidelines, and related procedures.
- Map coverage across business units, key functions, and critical systems.
- Identify overlaps, gaps, conflicts, and inconsistencies within existing security requirements.
- Evaluate policies against major business risks and relevant threat scenarios.
- Assess policy clarity, enforceability, auditability, and alignment with organisational needs.
- Define ownership, approval workflows, review cadence, and policy exception processes.
- Implement versioning and change history, ensuring consistent periodic policy reviews.
- Create a tiered architecture defining policies, standards, procedures, and guidelines.

vCISO (Virtual Chief Information Security Officer) and Support Service

The Virtual CISO service provides strategic leadership and guidance for your cybersecurity program without the cost of a full-time executive. We help define security strategy, manage risk, and oversee compliance initiatives.

Key Features include:

- Provide experienced executive cybersecurity leadership flexibly to support organisational needs.
- Serve as organisational CISO or extend existing leadership with expertise.
- Develop and own the organisation's cybersecurity strategy, roadmap, and priorities.
- Align security strategy to business objectives and organisation's risk appetite.
- Establish a cyber risk management framework supporting prioritisation and decision-making.
- Develop governance, policy structures, and a robust security operating model.
- Deliver board and executive reporting on cyber risk and posture.
- Provide oversight for incident readiness planning and coordinated response activities.
- Oversee third-party and supply chain security risks, controls, and performance.
- Provide regulatory guidance and compliance advisory support across security activities.
- Lead security awareness initiatives and foster a strong organisational culture.
- Provide budget guidance and prioritise security investments for maximum impact.
- Support vendor evaluations and guide technology selection for security needs.
- Oversee security assessments, audits, and remediation programmes ensuring effective outcomes.
- Coordinate IT, security, risk, compliance, and business teams for alignment.
- Provide ongoing advisory services, coaching, guidance, and informed decision support.
- Offer flexible engagement models including part-time, retainer, or project support.

Cyber Essentials / Cyber Essentials Plus and consultancy

PTPs consultancy and assessment services help organisations achieve Cyber Essentials and Cyber Essentials Plus certifications, strengthening baseline security controls and demonstrating commitment to cybersecurity.

Consultancy

PTP will provide a spreadsheet version the Cyber Essentials questions via email.

The approach will consist of:

- Customer completes an initial 'first pass' of the spreadsheet and the responses where possible. Any questions which are unclear should be left blank for review.
- The PTP consultant will review the initial spreadsheet version responses and annotate in preparation for a review interview.
- Interview between customer and PTP to validate responses and provide additions where required.
- PTP will then complete a final run through of the responses and check against the current marking guide to confirm a likely passing status.
- Assuming no remediation is required, a final wash up call will be held to agree next steps for client and arrange Pervade Portal access.
- If remediation is required a statement of work (SoW) will be produced, that PTP can provide support consultancy if required at an additional cost to be agreed.

Cyber Essentials

The client proceeds with completion via Pervade Portal and provides the scope and information there.

- A window of 48 business hours is available for amending CE Questionnaires if a fail is attained.
- If the organisation fails after 2 attempts, they must wait 1 month before re-applying.

Cyber Essentials Plus

Once a pass confirmation is attained, the client will proceed with appropriate external and internal testing to further validate compliance with Cyber Essentials and, therefore, attaining a Plus Status.

- CE Plus must be undertaken within 3 months of passing CE.
- The organisation being tested for CE Plus must have already achieved the Cyber Essentials self-assessment and the scope for the self-assessment must be the same as the scope for the CE Plus test.
- A window of 30 days is available for remediation and retesting after an initial CE Plus fail. The assessor must retest any specific issue identified and confirm it is resolved before issuing a certificate.
- If the client takes longer to remediate an issue, the whole CE Plus assessment must be carried out again by the assessor.

PCI DSS Services (can also be a Managed Service)

PTP Offer the following services:

- **PCI Design and Architecture Review** - To provide a review of a proposed implementation or change that may impact applicable PCI DSS requirements.

- **PCI Scope Review** - Prior to completion of an onsite QSA led review for PCI DSS compliance, PTP recommend completing a Scope review and Gap analysis

- **PCI DSS Task Remediation Service -** Working alongside technical, security, and operational teams to clarify remediation requirements, implement or improve controls, and ensure remediation activities align with PCI DSS intent. The service is flexible, and risk based, supporting both technical and procedural remediation activities across the cardholder data environment.

- **PCI Level 1 ROC Assessment** - A Level 1 Qualified Security Assessor (QSA) assessment, is undertaken to produce a Report on Compliance (ROC) and Attestation of Compliance (AOC) to meet reporting requirements for their acquiring bank(s).

- **PCI DSS SAQ Assistance & Validation Service -** designed to support organisations in accurately completing and submitting their applicable PCI DSS Self-Assessment Questionnaire (SAQ).

PCI Design and Architecture review

Scope: PTP will start with a review of the environment to include:

- Available physical / logical network diagrams.
- Design or architecture documentation.
- Review of any current in scope Cardholder Data Environment (CDE), and impact to the CDE from the proposed implementation or changes.

Approach: PTP will support our clients with their compliance requirements, the following steps will be followed:

Initial Review Process

- Review available documentation prior to initial session
- Onsite workshop with representation from IT, Network , Application teams as well as system end users to confirm processes.
- Creation of documentation including dataflows and network diagrams if these are not already available.

Follow Up Review

- PTP will support our clients review the initial recommendations and arrange any required internal peer review with other teams to verify details.
- Follow up call with PTP to discuss report and any next steps that may be required such as design changes or control remediation.

PCI Scope Review

The scope for the review covers all payment channels for any Merchant IDs owned by PTP will support our clients. This allows PTP to:

- Review the current payment channels and dataflows, to properly identify all in scope personnel, systems, and processes.
- Review all Third Party Service Providers (TPSPs) engaged to ensure their supporting compliance is correctly documented
- The correct applicable PCI requirements, and evidence that will be needed to successfully complete an assessment process.
- Identify any areas of remediation that may be required to implement prior to the assessment.
- Produce a documented gap analysis using the Prioritized Approach Report (PAR) template, showing any required actions and suggested timescales.

Approach: To support the review process, a site visit will be completed to review applicable requirements. The audience for this review should include the following business areas:

- IT Management
- Development
- Facilities / Building Management
- HR
- Finance
- Customer Service / Support

Representation from most teams will not be required for the entire day, we just need to ensure staff are contactable during the day for questions if needed.

Any in scope third parties may also need to provide information. If there is a significant number of controls covered by a TPSP, it may be advisable to have a representative onsite or booked for a call on the same day. Instances where the TPSP provides managed services for IT, typically require several interactions throughout the visit.

As potential architectural changes can be used to simplify scope, the onsite review will include a design exercise with applicable controls being considered for both existing and new requirements. This can potentially reduce the compliance burden for the assessment.

PCI DSS Task Remediation Service

PTPs PCI DSS Task Remediation Service provides targeted, hands-on support to help organisations remediate specific PCI DSS compliance gaps identified through an SAQ, internal review, or third-party assessment. The service focuses on addressing defined remediation tasks rather than performing a full reassessment, enabling efficient progress toward compliance.

We work alongside technical, security, and operational teams to clarify remediation requirements, implement or improve controls, and ensure remediation activities align with PCI DSS intent. The service is flexible and risk-based, supporting both technical and procedural remediation activities across the cardholder data environment.

Key Benefits

- **Accelerated Remediation**
  Address PCI DSS gaps more quickly through focused expertise and clearly defined remediation actions.
- **Practical, Actionable Support**
  Translate PCI DSS requirements into achievable technical and operational tasks aligned to your environment.
- **Reduced Compliance & Audit Risk**
  Ensure remediation activities adequately address underlying control weaknesses rather than surface-level fixes.
- **Resource Augmentation**
  Supplement internal teams with specialist PCI DSS knowledge without the overhead of long-term resourcing.
- **Improved Control Maturity**
  Strengthen security controls and processes in a way that supports ongoing compliance and operational resilience.

Service Deliverables

- Remediation Task Scoping & Prioritisation
  Review and confirmation of in-scope remediation tasks, aligned to specific PCI DSS requirements and risk severity.
- **Remediation Action Guidance**
  Detailed guidance on required control improvements, including technical, procedural, or governance-related actions.
- **Hands-On Remediation Support (Where Applicable)**
  Practical assistance with implementing controls such as policy updates, process changes, configuration guidance, or evidence structuring.
- **Validation of Remediation Outcomes**
  Review of remediated controls and supporting evidence to confirm alignment with PCI DSS intent.
- **Remediation Status Tracking**
  Clear visibility of completed, in-progress, and outstanding remediation tasks.

- **Remediation Summary Report**
  A concise summary documenting remediation activities performed, outcomes achieved, and any residual risks or follow-up actions.

PCI Level 1 ROC Assessment

Scope: The reporting is produced following onsite and remote reviews for all in scope payment channels, based on Merchant IDs owned by PTP will support our clients.

The assessment will also consider any Third-Party Service Providers (TPSPs) that provide outsourced or supporting services for those payment channels.

Approach: Pen Test Partners (PTP) will provide PCI QSA services to complete the following stages:

Stage 1
Complete a high-level workshop to review in scope controls. The purpose of this activity is to ensure the business has correctly scoped their payment channels, and appropriate controls are in place. This stage considers:

- What is in place now and could be assessed. Typically, technical controls are in place (such as password complexity / unique user IDs / patching etc.) but some supporting documentation and processes may need to be remediated before final assessment.

- Agree dates for completion of any remediation items prior the onsite assessment being scheduled.

Stage 2
Consists of several activities:

- Review of the payment channel environment(s) and capture screenshots / log files etc. as evidence. PTP will also complete interviews with key staff to support the assessment.
- Requests for any documentation, to be stored with the report and answer documentation specific controls.
- (offline) – PTP compile the detailed responses in the ROC report, including overview of the environment and creating any required diagrams / data flows in Visio to go in the report.
- (offline) – Entire report is QA reviewed by another QSA to confirm report is defensible and accurate (a PCI SSC requirement)
- PTP finally send over an AOC (Attestation of Compliance) and ROC report for COMPANY NAME to review and sign, and PTP to countersign.

PCI DSS SAQ Assistance & Validation Service

Our **PCI DSS SAQ Assistance & Validation Service** is designed to support organisations in accurately completing and submitting their applicable PCI DSS Self-Assessment Questionnaire (SAQ). The service provides expert guidance throughout the SAQ process, helping to interpret PCI DSS requirements, validate responses against evidence, and reduce the risk of errors or misstatements that could lead to non-compliance.

We work collaboratively with key stakeholders to assess the organisation's cardholder data environment, confirm the correct SAQ type, and provide practical, risk-based advice aligned to PCI DSS expectations. This service does not replace internal accountability for compliance, but ensures the SAQ is completed with confidence, consistency, and clarity.

Benefits

- **Reduced Compliance Risk**
  Minimise the likelihood of incorrect responses, unsupported assertions, or misinterpretation of PCI DSS requirements.
- **Expert Guidance**
  Leverage PCI DSS subject-matter expertise to interpret requirements and apply them correctly to your environment.
- **Time & Effort Savings**
  Streamline the SAQ process through structured workshops, clear evidence expectations, and focused remediation guidance.
- **Improved Assurance**
  Increase confidence for internal stakeholders, acquiring banks, and payment brands that the SAQ accurately reflects your security posture.
- **Audit-Ready Outcomes**
  Establish clearer documentation and evidence practices to support future PCI DSS assessments or transition to a QSA-led assessment, if required

Deliverables

- **SAQ Type Confirmation**
  Validation of the applicable SAQ type based on your cardholder data environment and payment flows.
- **SAQ Completion Support**
  Guided walkthrough of each relevant SAQ requirement, including clarification of intent and applicability.
- **Evidence Review & Validation**
  High-level review of supporting documentation and artefacts to validate SAQ responses for consistency and adequacy.
- **Gap Identification & Recommendations**
  Identification of gaps or areas of concern, with pragmatic recommendations to address non-compliant or partially compliant controls.
- **Validated SAQ Output**
  A completed or reviewed SAQ, ready for submission, with documented assumptions and notes where applicable.

ISO 27001 Services (can also be a Managed Service)

The scope of an engagement is based on the planned scope for the formal certification, and this is based on the requirements of the business. Typically 20 to 100 days.

Scope can either be an entire business and all aspects of its operations, or a sub set such as a specific location or department / function.

Core Components:

- Risk assessment and treatment
- Security Policy and Procedures
- Management of the company
- Asset management
- Access control
- Incident management
- Compliance with legal & regulation requirements
    - Annex 1 controls grouped into 4 themes: Organisation, People, Physical and Technology

ISO 27001 certification support approach

The scope of the support activity includes:

- Creation of applicable support policies, processes and work instructions.
- Review of existing policy and process documentation, to integrate with required ISMS documentation.
- Meeting mandatory clauses within ISO27001:2013 (4-10), and any applicable supporting processes.
- Risk assessment methodology and identification of suitable controls from Annex A of the standard.
- Training staff internally to conduct required activities such as:
    - Risk assessments and risk treatment.
    - Internal audit program.
    - Handling identified non-conformities.
    - Management of security incidents.
- Planning support resources including:
    - Asset management
    - Security awareness training
    - Third party management

Key Features include:

- Conduct baseline review against ISO 27001 clauses and Annex A controls.
- Assess evidence and artefacts including policies, procedures, registers, and assets.
- Define Information Security Management System scope for organisational applicability.
- Author policy suites and standards covering risk, access, incidents, assets.
- Establish ISMS governance roles, RACI structures, workflows, and review cadence.
- Facilitate workshops identifying assets, threats, vulnerabilities, and organisational exposures.
- Create risk register and treatment plans aligned with business priorities.
- Develop Statement of Applicability including justifications and identified exclusions.
- Design and enable controls across people, processes, technology, and governance layers.
- Integrate ISMS with NIST, CIS, PCI DSS frameworks where relevant.

- Plan and execute internal first-party ISMS audits effectively and consistently.
- Prepare management review inputs, metrics, summaries, and corrective action plans.
- Define supplier risk assessments and due diligence evaluation criteria comprehensively.
- Map contractual controls and deliver clear supplier assurance reporting outputs.
- Monitor critical vendors and services through continual oversight and evaluations.
- Align incident response processes and playbooks directly with ISMS requirements.
- Coordinate business continuity planning activities and facilitate organisational testing.
- Integrate lessons learned into corrective and preventive action processes.
- Conduct pre-audit readiness checks and prepare required evidence packages.
- Liaise effectively with certification auditors during Stage One and Two.
- Support remediation of nonconformities and prepare for surveillance audits.
- Deliver role-based ISMS training for leadership, administrators, and users.
- Create ISMS onboarding materials, communications plans, and refresher schedules.
- Provide structured knowledge transfer to internal ISMS owners and teams.
- Develop improvement backlog and roadmap spanning twelve to twenty-four months.
- Perform periodic risk reassessments and maintain accurate applicability statements.
- Offer ongoing advisory governance oversight aligned with vCISO service models.

UK Defence Cyber Certification (DCC)

We assist defence suppliers in achieving UK DCC compliance, ensuring adherence to MOD cybersecurity requirements and safeguarding sensitive defence-related data.

Key Features include:

- Baseline review against MOD Cyber Security Model v4 and standards.
- Map organisation to appropriate DCC level based on MOD risk.
- Confirm Cyber Essentials prerequisites with clear evidence expectations where applicable.
- Implement required organisational and technical controls for each DCC level.
- Compile defensible evidence for assessor review including policies and configurations.
- Manage flow-down to subtiers aligned with CSM and DEFCON requirements.
- Create prioritised remediation backlog and CIP timelines to reach compliance.
- Plan annual reassessments, evidence refresh cycles, and internal audit cadence.
- Maintain supplier cyber protection familiarity including legacy SAQ knowledge throughout.
- Support continuous alignment with CSM v4 and uplifted defence standards.

ISO 42001 Compliance

Our ISO 42001 service helps organisations implement AI governance frameworks, ensuring ethical, secure, and compliant use of artificial intelligence technologies.

Key Features include:

- Baseline assessment against ISO/IEC 42001 requirements and control objectives
- Identification of in scope AI systems, models, data pipelines, and suppliers
- Gap analysis across governance, risk, ethics, and technical controls
- Definition of AIMS scope aligned to business use of AI
- Design of AI governance structure, roles, and responsibilities
- Integration of AIMS with existing ISMS / GRC frameworks (e.g. ISO 27001)
- AI specific risk identification and assessment (bias, explainability, safety, misuse, data quality)
- Definition of AI risk criteria, tolerances, and treatment options
- Creation of an AI risk register and treatment plans
- Development or alignment of AI specific policies (AI use, ethical AI, data usage, human oversight)
- Control design covering model lifecycle, training, validation, deployment, and monitoring
- Alignment to regulatory and ethical expectations
- Governance controls for design, development, testing, deployment, and retirement of AI systems
- Change management and version control for models and datasets
- Human in the loop and oversight mechanisms
- Assessment of third party AI tools and service providers
- Contractual and assurance requirements for AI suppliers
- Ongoing monitoring of outsourced or embedded AI capabilities
- Definition of KPIs and KRIs for AI risk and performance
- Internal audit and assurance planning for AIMS effectiveness
- Role based AI governance and risk awareness training
- Guidance for developers, data scientists, product owners, and leadership
- Cultural alignment to responsible and ethical AI use
- ISO 42001 certification readiness and evidence preparation
- Support through Stage 1 and Stage 2 audits
- Ongoing advisory, AIMS maintenance, and maturity improvement