



**SAFEHARBOUR
SECURITY**

Service Definition Document

ISO Consultancy Services

Service: ISO Consultancy Services

Supplier: Safe Harbour Security

Date: January 2026

Version	Approved by
1.0	Gary O'Brien

Service Description Document

What is ISO Consultancy

Safe Harbour Security provides adaptive ISO consultancy services, offering requirements-aligned and pragmatic guidance across information security, privacy, quality, cloud security, incident response, and business continuity standards.

Our approach is flexible, environment-appropriate, and fit-for-purpose, supporting organisations in achieving, maintaining, and enhancing compliance through expert assessments, gap analysis, implementation support, and continual improvement planning.

Engagements are guided by recognised international standards and best practice, but remain adjustable to each organisation's operational context, regulatory obligations, and strategic priorities.

Business Continuity & Data Protection

All consultancy engagements are managed with secure handling of client information, ensuring confidentiality, integrity, and availability of documentation and deliverables.

Data Access & Security:

- Client data is accessed strictly on a need-to-know basis, protected in line with ISO 27001 principles, and remains the client's property.

Data Retention & Transfer:

- Raw testing data, credentials, and evidence are retained for up to 90 days following delivery of the final report. Final reports are retained for up to 24 months for contractual, audit, and quality assurance purposes. Clients may request secure copies or transfer of data upon completion.

Data Backup:

- All client data is stored on secure systems with redundant backup measures to prevent loss and support business continuity.

Continuity Assurance:

- Safe Harbour maintains contingency measures to ensure uninterrupted consultancy, with adaptable remote or on-site approaches and regular progress updates.

Compliance:

- All activities are conducted in accordance with ISO standards, GDPR, and industry best practices, embedding confidentiality, data protection, and operational integrity throughout.

Service Features

- ISO/IEC 27001:2022- Information Security
- ISO/IEC 27017:2015- Cloud Security
- ISO/IEC 27035- Incident Management
- ISO 22301:2019- Business Continuity
- ISO/IEC 27701:2019- Privacy Management
- ISO 9001:2015- Quality Management
- ISO/IEC 42001:2023- AI Management Systems

Service Description Document

Service Benefits

- Support adaptive security practices, improving governance and organisational readiness for risks.
- Enhances configurable and secure cloud operations, aligning controls with organisational cloud strategy.
- Improves environment-appropriate readiness, response, and learning from security events.
- Strengthens flexible continuity planning and operational resilience during disruptions.
- Supports adaptable personal data governance, ensuring compliant and trustworthy privacy practices.
- Enhances scalable process consistency and performance, supporting continual improvement across the organisation.
- Supports safe, ethical, and responsible AI deployment

Onboarding

Before each engagement, Safe Harbour Security works with clients to establish objectives/key priorities, define scope, and prepare access and documentation.

Onboarding typically includes:

- Initial scoping call
- Definition of engagement objectives and rules of engagement
- Identification of in-scope processes and systems
- Agreement of consultancy schedules and contact points
- Provisioning of access to documentation or systems (if required)
- Agree timeframes and key milestones
- Define organisational roles and responsibilities
- Build and develop management system around specified ISO Standard.

Offboarding & Exit Support

At engagement conclusion, Safe Harbour Security ensures clients can act on findings and securely manage deliverables.

Offboarding includes:

- Fully developed management system built around specified ISO standard.
- Certification readiness guarantee.
- Specific to ISO/IEC 27001 control branches: ISO Stage 1 and Stage 2 review and debrief sessions.
- Support for remediation and improvement queries.

Service Constraints

To deliver secure and effective consultancy:

- Engagements may be scheduled according to operational availability
- Access to certain documentation or systems may be required
- Client approval required for specific assessments or observations
- Consultancy scope may be adjusted based on evolving requirements
- Certification bodies to be selected by client.
- Safe Harbour Security has no control over availability/ certification dates of the chosen certification body.
- MSPs are to be instructed and managed by client.
- Additional licensing and systems to be purchased by client.

Service Description Document

Service Levels

Safe Harbour Security ensures consultancy delivery is reliable, responsive, and aligned to client needs.

Service levels include:

- Consultancy availability as per agreed schedule
- Standard support hours: 09:00–17:00, Monday–Friday (UK)
- Immediate notification for critical issues affecting delivery
- Reports and recommendations delivered within agreed timelines

Post-Certification Support

After certification, clients can access support to clarify findings and integrate improvements.

Support includes:

- Review sessions to discuss outcomes and recommendations
- Assistance with prioritisation of improvements
- Clarification of technical or operational points
- Optional follow-up consultancy (vCISO) or validation reviews

Technical Requirements

To deliver ISO consultancy services effectively and safely, Safe Harbour Security may require certain technical resources, access, and organisational information from the client. These requirements ensure consultancy activities are conducted efficiently, securely, and in a manner that aligns with the client's operational environment.

Key technical requirements may include:

- Access to relevant Sharepoint, Google Drive or secure storage
- Organisational context for existing management systems, controls, and risk registers
- Availability of subject matter experts, system owners, or other stakeholders for interviews and workshops
- Access to relevant IT systems, applications, or cloud environments where in-scope processes are implemented
- Provision of data, architecture diagrams, or system maps to support gap analysis and improvement recommendations
- Any client-specific tools or platforms necessary to perform assessments or validate compliance
- Flexibility to adapt engagement approach based on the level of access, system complexity, and client operational priorities

Service Description Document

Outage & Maintenance Management

Safe Harbour Security recognises that consultancy engagements may require the availability of client systems, personnel, or operational information. To minimise disruption and ensure services are delivered safely and effectively, we implement clear processes for managing planned or unplanned outages and maintenance events.

Management measures include:

- Scheduling consultancy activities around normal operations and maintenance windows to reduce business impact
- Pausing or adjusting engagement activities if critical organisational issues arise or access is restricted
- Proactive communication with client stakeholders regarding any potential disruptions, changes, or delays
- Logging and tracking significant events during consultancy to maintain auditability and transparency
- Flexible planning to accommodate urgent client priorities while maintaining the integrity of the engagement

Hosting Locations

Safe Harbour Security does not host or operate client systems as part of our ISO consultancy service. All work products, documentation, and engagement outputs are securely stored within controlled UK and EU environments, ensuring compliance with data protection regulations and organisational security policies.

Data Access Upon Exit

Clients retain full ownership of all engagement deliverables and supporting evidence. Safe Harbour Security ensures a smooth and secure handover at the conclusion of each consultancy engagement.

Key provisions include:

- Provision of all reports, assessments, and supporting documentation in agreed formats
- Secure transfer of engagement data to client systems or designated storage locations
- Optional destruction of all retained data in a verifiable, secure manner upon client request
- Written confirmation provided for any securely deleted or returned materials where required.
- Continued support to clarify findings, methodologies, or recommendations during the transition phase

Security

Certified to ISO/IEC 27001:2022 and Cyber Essentials Plus, Safe Harbour Security applies a rigorous security framework across all consultancy engagements to protect client information, ensure confidentiality, and uphold deliverable integrity.

Key security measures include:

- Encryption of all engagement data at rest and in transit using industry-standard protocols
- Secure handling of credentials, documentation, and supporting evidence, with strict access controls
- Segregated and auditable working environments to maintain data privacy and integrity
- Personnel screening, adherence to professional standards, and security awareness training for all staff
- Documented procedures for managing potential security incidents, including mitigation, reporting, and follow-up
- Flexibility to align security measures with client-specific policies and operational requirements



**SAFEHARBOUR
SECURITY**

✉ info@safeharboursecurity.com

🌐 www.safeharboursecurity.com

📍 Catalyst Innovation Building, Bay Rd, Londonderry BT48 7TG

🌐 @ SafeHarbourSecurity