



**SAFEHARBOUR
SECURITY**

Service Definition Document

Governance, Risk & Compliance

Service: Governance, Risk & Compliance

Supplier: Safe Harbour Security

Date: January 2026

Version	Approved by
1.0	Gary O'Brien

Service Description Document

What is Governance, Risk & Compliance (GRC)

Safe Harbour Security delivers pragmatic, adaptive GRC services, supporting organisations in aligning governance, risk management, and compliance with industry standards and regulatory obligations.

Our approach is flexible, fit-for-purpose, and scalable, covering strategic advisory, operational risk assessment, compliance planning, and ongoing monitoring. Services are designed to be requirements-aligned and environment-appropriate, helping organisations strengthen security, manage risk, and demonstrate compliance across multiple frameworks including NIST, GDPR, PCI-DSS, SOC 2, and the Cyber Assessment Framework (CAF 4.0).

Business Continuity & Data Protection

Engagement Management:

- All consultancy activities are conducted 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, safeguarded according to ISO/IEC 27001 principles, and remains the client's property.

Data Retention & Transfer:

- Raw evidence, credentials, and working data are retained for up to 90 days post-delivery of the final report. Final reports are retained for up to 24 months to support contractual, audit, and quality assurance requirements. 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 continuity.

Continuity Assurance:

- Safe Harbour implements contingency plans to ensure uninterrupted consultancy, using adaptable remote or on-site approaches and providing regular progress updates.

Regulatory Compliance:

- All activities align with ISO standards, GDPR, and industry best practices, embedding confidentiality, data protection, and operational integrity throughout all consultancy engagements.

Service Description Document

Service Features

- vCISO Service
- vDPO Service
- GDPR Compliance
- CE & CE+ Consultancy
- SOC 2
- Cyber Security Third Party Risk Assessment
- Cyber Assessment Framework (CAF 4.0)
- NIST
- NIS2 Directive
- PCI-DSS

Service Benefits

- Provides pragmatic strategic security guidance and oversight
- Supports adaptive personal data protection governance
- Strengthens regulatory alignment and privacy management practices
- Enhances risk management and operational compliance capabilities
- Improves trust, control assurance and reporting practices
- Strengthens vendor oversight and reduces exposure to external risks
- Provides flexible, standards-aligned cyber risk assessment and advisory
- Supports adaptable risk management and security practices
- Strengthens EU regulatory alignment and cybersecurity governance
- Enhances payment security compliance and operational resilience

Onboarding

Onboarding ensures clients are fully prepared for the engagement, with clear objectives, scope, and access requirements. This process establishes a foundation for successful consultancy delivery.

- Initial scoping workshops to define engagement objectives
- Identification of in-scope systems, processes, and regulatory requirements
- Establishment of points of contact and engagement schedule
- Access provisioning to documentation, systems, or stakeholders as required

Service Description Document

Off-boarding & Exit Support

Safe Harbour Security ensures that clients can act on findings and recommendations effectively after engagement completion. Our offboarding process facilitates a smooth transition and ensures all deliverables are securely handed over.

- Delivery of assessment reports, recommendations, and supporting documentation
- Debrief sessions to review findings and next steps
- Guidance for remediation prioritisation and follow-up activities
- Secure return or deletion of client data upon request

Service Constraints

This section outlines the practical constraints that may influence the delivery of GRC services, allowing clients to plan and prioritise accordingly.

- Engagements are delivered according to agreed schedules
- Certain assessments may require access to systems, personnel, or documentation
- Scope may be adjusted as client priorities or regulatory obligations evolve
- IACPA accredited body to be chose by the client for development of SOC2 report

Service Levels

Safe Harbour Security commits to providing bespoke consultancy services in a reliable and responsive manner. This section describes the service levels clients can expect.

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

Post Engagement Support

After-sales support provides clients with clarity and guidance to act on findings and maintain compliance improvements over time.

- Review sessions to clarify findings and recommendations
- Ongoing advisory for remediation or compliance improvements
- Optional follow-up assessments to validate remediation efforts
- Access to security and GRC specialists for clarifications during support hours

Service Description Document

Technical Requirements

Technical requirements outline the resources, access, and organisational context required to conduct effective consultancy engagements.

- Access to relevant policies, procedures, and process documentation
- Organisational context for existing governance, risk, and compliance controls
- Availability of stakeholders for interviews, workshops, and validations
- Access to systems, logs, or platforms where applicable for assessment purposes
- Flexibility to adapt the engagement approach based on client environment and priorities

Hosting Locations

All engagement deliverables and documentation are stored securely in controlled UK/EU environments, ensuring compliance with regulatory and client-specific requirements.

- Encrypted storage and access-controlled repositories for client deliverables
- Compliance with data protection requirements and client-specific hosting preferences
- Audit-ready processes for handling and transferring engagement deliverables

Outage & Maintenance Management

This section describes how Safe Harbour Security manages potential disruptions, maintenance, or changes during engagements, to maintain continuity and integrity of service delivery.

- Engagement activities scheduled to minimise business disruption
- Pausing or adjusting work if critical operational issues arise
- Proactive communication of potential delays or changes
- Logging and tracking of significant events to maintain transparency
- Flexible planning to accommodate urgent client priorities while maintaining engagement integrity

Service Description Document

Data Access Upon Exit

Safe Harbour Security ensures clients retain full control over engagement outputs at the conclusion of an engagement.

- Full ownership of all reports and supporting evidence retained by client
- Secure transfer of all engagement materials in agreed formats
- Optional secure deletion of retained data with confirmation
- Continued support to clarify findings or recommendations during the transition phase
- Assurance that no client information is retained beyond agreed engagement timelines

Security

This section details the measures Safe Harbour Security employs to protect client information and maintain a secure consultancy environment.

- Encryption of engagement data at rest and in transit
- Secure handling of credentials, reports, and supporting evidence
- Segregated, auditable working environments to maintain data privacy and integrity
- Personnel screening and adherence to professional standards
- Flexible alignment of security measures with client policies
- Documented procedures for managing potential security incidents, including mitigation and reporting



**SAFEHARBOUR
SECURITY**

✉ info@safeharboursecurity.com

🌐 www.safeharboursecurity.com

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

🌐 @ SafeHarbourSecurity