Evalian Limited

Cyber, Data Protection & Resilience Consultancy Service Description

26 January 2026

CREST MEMBER

CREST INCIDENT MANAGEMENT Incident Exercising

CREST INCIDENT MANAGEMENT Incident Response

Assured Service Provider in association with National Cyber Security Centre Cyber Incident Response: Standard Level

Assured Service Provider in association with National Cyber Security Centre Cyber Incident Exercising

ISO 27001 INFORMATION SECURITY MANAGEMENT

ISO 9001 QUALITY MANAGEMENT

CERTIFICATION BODY CYBER ESSENTIALS PLUS

1. Service Summary

Evalian's consultancy services cover cyber security, data protection and organisational resilience. Our services can be delivered based on scoped consultancy days, fixed-price outcome focused engagements, or as part of an ongoing subscription service with agreed hours for call-off.

Evalian is an award-winning cybersecurity provider, certified to ISO 27001, ISO 9001, ISO 22301 and Cyber Essentials Plus. We are an NCSC Assured Service Provider for Cyber Incident Response and Cyber Incident Exercising and hold additional accreditations from the NCSC and CREST across advisory, penetration testing, and incident response services.

2. Consultancy Services

2.1. Cyber Security Consultancy

Evalian's cyber security consultancy covers the following services:

- Cyber Security Gap Analysis & Improvement
- Cyber Security Compliance with Laws, Regulations & Standards
- Cyber Security Governance, Risk & Compliance
- Cyber Security Incident Response
- Cyber Security Incident Exercising & Simulation
- Supply Chain Security Risk Management
- Cyber Security Awareness Training
- Cloud Secure Configuration Assessments
- NCSC CAF Readiness & Auditing
- Cyber Essentials Plus Readiness & Assessment
- ISO 27001 Certification Gap Analysis & Readiness
- SOC 2 Attestation Gap Analysis & Readiness
- Cyber Security Leadership & Programme Management
- Bespoke Cyber Security Consultancy
- CREST Accredited Penetration Testing
- CREST Accredited Vulnerability Assessments

2.2. Data Protection & AI Governance Consultancy

Evalian's data protection and AI governance consultancy covers the following services:

- UK & EU GDPR Gap Analysis & Compliance Improvement
- UK & EU GDPR Compliance Auditing
- Subject Access Request Support

- DPIA Preparation & Review
- PECR & Electronic Marketing Compliance
- International Data Transfer Compliance
- Privacy Notice, Policy & Processing Agreement Review & Improvement
- Outsourced Data Protection Officer (DPO)
- AI Governance & EU AI Act Gap Analysis & Compliance Improvement

2.3. Organisational Resilience Consultancy

- Evalian's organisational resilience consultancy covers the following services:
- Business Impact Analysis Preparation & Review
- Business Continuity Planning
- Business Continuity Auditing
- Business Continuity Exercising & Simulation
- ISO 22301 Certification Gap Analysis & Readiness

3. Example Methodology

3.1. Advisory Services

Whilst the exact approach followed depends on the nature of the consultancy being provided and the client's objectives and timelines, our typical consulting methodology is as described in this section.

We start consulting engagements with discovery meetings and workshops with your stakeholders. Where the service includes a gap analysis or health check, these sessions will be used to gather the information required to assess your level of compliance or maturity and to contribute to the report and recommendations.

In all cases, irrespective of whether a gap analysis is included, we use the discovery sessions to build an understanding of the client's organisation, including their risk appetite, culture, critical assets, organisational objectives and plans. This is important in helping us tailor the service and our deliverables to the client's needs and expectations.

Thereafter we will schedule meetings with the client's key stakeholders. These will differ according to the nature of the consultancy we are providing. Unless onsite work is agreed, we will facilitate discovery meetings using Microsoft Teams or the client's preferred collaboration platform if Teams is problematic.

During meetings with stakeholders, we take notes, and may ask for supporting documents to be sent to us to review. After meetings we may have follow-up queries which we will email to stakeholders. Discovery meetings typically require one hour. Meetings with two or more stakeholders sometimes require more time.

We typically also ask the client to share all related documents (policies, procedures, records and similar) with us in advance. We use these to carry out a desk-based review to understand the maturity of current policies and to identify areas for improvement, where in scope of the engagement.

Documents can be securely shared with us through our client portal. Alternatively, we can use the client's secure document sharing tools if preferred.

We classify all client documents as Confidential Information as set out in our Information Classification Policy (a copy of which can be provided on request). Least privilege access is applied to client documents.

3.2. Penetration Testing

Our approach to penetration testing is consistent with industry best practice methodologies, including OWASP and OSSTM. During testing we work through the following steps:

- **Initial Checks**: Before formal testing starts, we will perform checks to ensure that systems and hosts exist, are accessible and are running as expected.
- **Discovery**: We will carry out reconnaissance searches to collect information about the target of the type an attacker would seek.
- **Enumeration:** We scan all hosts and services using multiple tools to gather information about the target systems and to identify vulnerabilities in the same way that an attacker would.
- **Exploitation**: Using the information gathered and vulnerabilities identified, we will use manual exploit techniques against the target systems.

Upon completion of testing, the tester will prepare their report, covering the following topics:

- Management Summary
- Test Information
- Test Summary
- Technical Report
- Vulnerability Details & Remediation Advice

Reports are delivered through SecureIQ, Evalian's dedicated penetration test reporting and vulnerability tracking application. PDF versions of reports can be downloaded from SecureIQ. We can also provide traditional PDF reports for clients who would prefer not to use SecureIQ.