E2E SC

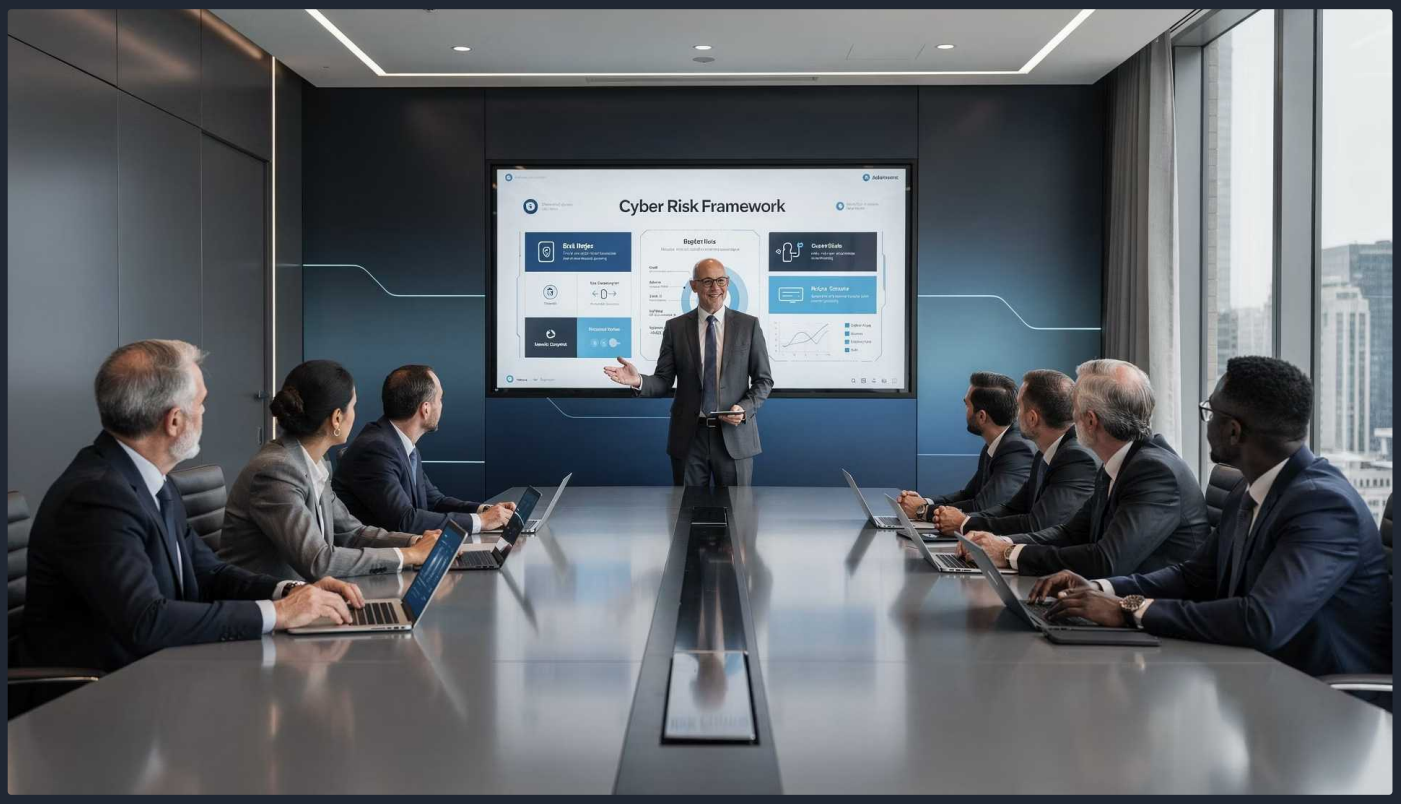
Governance, Risk and Compliance Advisory & Support Services

G-Cloud 15 Service Definition - Version 1.0 - January 2026

E2E Security Consulting Ltd

Service Overview

E2E Security Consulting Ltd (E2E SC) delivers Governance, Risk & Compliance (GRC) advisory and support services designed for organisations that need security governance to produce accountable decisions, not just compliance documentation. Our approach recognises that effective security risk management is fundamentally a governance challenge requiring senior ownership, clear accountability, and defensible decision-making—not simply a technical problem requiring more tools or processes.



Security Governance

Design and implement governance structures that establish clear accountability for cyber risk at appropriate organisational levels.

Risk Management

Enable senior leaders to understand which risks matter, which can be tolerated, and which require intervention.

Assurance & Compliance

Provide independent assurance that security controls are operating effectively and compliance obligations are being met.

Advisory Expertise

Support organisations in making informed, defensible decisions about risk where there are no perfect options.

We help organisations build security governance structures that work in practice: defining roles and responsibilities that are actually exercised, implementing risk management processes that inform genuine decisions, and establishing assurance mechanisms that provide boards and senior leaders with the confidence they need to discharge their accountability for cyber risk.

Decision-Grade Security and Risk Advisory

E2E Security Consulting specialises in decision-grade security and risk advisory. Our services are designed to support senior leaders, Accounting Officers, and boards in making informed, defensible decisions about risk—particularly where there are no perfect options.

We recognise that security governance is not about eliminating risk, but about making deliberate trade-offs between operational need, cost, resilience, and regulatory expectation. Our role is to make those trade-offs explicit, evidence-based, and accountable—rather than implicit, undocumented, or assumed.

Evidence-Based Decisions

Making trade-offs explicit and accountable with structured evidence

Withstanding Scrutiny

Decisions that hold up after incidents, audits, and inquiries

Independent Challenge

Providing senior leaders with objective advice before committing to action

This approach differentiates E2E Security Consulting from traditional framework-driven consultancies, which often focus on producing documentation rather than enabling confident decision-making. We understand how decisions are examined after incidents, audits, and inquiries—and we help clients make decisions that will withstand that scrutiny.

Why E2E Security Consulting

The GRC advisory market contains many capable firms. What makes E2E SC different is not that we know more about security frameworks or compliance requirements—it is that we approach security governance as a decision-making discipline rather than a documentation exercise. This philosophical difference produces materially different outcomes for our clients.

Governance That Works After We Leave

We design governance structures for sustainability: clear enough to be understood, practical enough to be followed, and embedded deeply enough to survive staff turnover and organisational change.

Connected to Business Decisions

Security considerations become part of how the organisation makes decisions rather than a separate compliance activity conducted in parallel.

Public Sector Accountability

Our team includes consultants with direct experience working within central government, local authorities, NHS organisations, and arm's length bodies.

Advisory Expertise with Technology

We combine deep advisory expertise with the ability to enable implementation through technology where appropriate, providing seamless integration between recommendations and execution.

Our staff hold security clearances up to Developed Vetting (DV) level, enabling us to support organisations handling the most sensitive information and operating in the most demanding security environments.

Core Service Capabilities

E2E SC delivers GRC advisory and support services across five integrated capability areas. Each capability can be engaged independently or combined into comprehensive transformation programmes depending on organisational needs and maturity.

Security Governance Design and Implementation

Design and implement security governance structures that establish clear accountability for cyber risk at appropriate organisational levels.

Security Risk Management

Enable senior leaders to understand which risks genuinely matter, which can be tolerated, and which require intervention.

Security Assurance and Compliance

Determine whether current security posture is acceptable, defensible, or requires remediation with supporting evidence.

Security Programme and Project Support

Ensure security implications are visible when architectural and investment decisions are being made.

Security Culture and Capability Development

Build internal judgement and expertise to sustain good security decisions independently.

Security Governance Design and Implementation

Our governance services provide confidence that security decisions are being made deliberately, reviewed appropriately, and supported by evidence that will withstand scrutiny. We design and implement security governance structures that establish clear accountability for cyber risk at appropriate organisational levels.

Board-Level Oversight

Define board-level oversight responsibilities and establish security committee structures with clear terms of reference

Role Definitions

Create role definitions for security leadership positions with clear accountability and authority

Governance Documentation

Develop security policies, standards, and procedures that satisfy regulatory expectations while remaining practical

Implementation Support

Facilitate governance committee establishment and coach senior leaders on their security responsibilities

Our governance designs address the full scope of security accountability: who owns security risk at board level, how security decisions are escalated and approved, what information boards need to discharge their oversight responsibilities, and how security governance integrates with broader corporate governance structures.

Security Risk Management

Our risk management services enable senior leaders to understand which risks genuinely matter, which can be tolerated, and which require intervention—providing the clarity needed to make confident, defensible decisions. We help organisations establish risk management capabilities that inform genuine decisions about security investment, risk acceptance, and control implementation.

01

Risk Appetite Definition

Workshops with senior leadership to define acceptable risk levels

02

Methodology Design

Risk assessment methodology development and documentation

03

Risk Register Development

Risk register design, population, and ongoing management support

04

Reporting Frameworks

Risk reporting framework development for boards and senior leadership

Our approach treats security risk management as a decision-support discipline. Risk assessments should enable informed choices about which risks to treat, accept, transfer, or avoid—not simply document threats and vulnerabilities for compliance purposes.

Security Assurance and Compliance

Our assurance services help organisations determine whether their current security posture is acceptable, defensible, or requires remediation—and provide the evidence needed to support that judgement. We provide independent assurance that security controls are operating effectively and compliance obligations are being met.

Control Assessments

Security control assessments against ISO 27001, NIST CSF, Cyber Essentials, CAF, and sector-specific requirements

Gap Analysis

Compliance gap analysis and remediation planning with prioritised recommendations

Certification Support

Preparation and support for ISO 27001, Cyber Essentials Plus, and other certifications

Regulatory Compliance

Assessments for NIS2, DORA, and sector-specific regulatory requirements

Our assurance approach emphasises practical effectiveness over theoretical compliance. We assess whether controls actually reduce risk rather than simply whether documentation exists. This means testing controls in operation, interviewing staff who operate them, and examining evidence of control effectiveness.

Security Programme and Project Support

Our programme services ensure security implications are visible when architectural and investment decisions are being made—not discovered after commitments have been made and options have closed. We embed security expertise within programmes and projects to ensure security is designed in from the outset rather than retrofitted after key decisions have been made.

Programme Board Representation

Security representation on programme boards to ensure visibility at decision points

Architecture Review

Security architecture review and challenge of design decisions

Threat Modelling

Threat modelling workshops to identify security risks early

Assurance Gates

Security assurance gate reviews at key programme milestones

Early engagement prevents the costly rework that occurs when security issues are discovered late in delivery. We help programme teams understand security implications of architectural choices, identify security risks that could threaten programme success, and implement proportionate security controls that do not unnecessarily impede delivery.

Security Culture and Capability Development

Our capability development services ensure organisations can sustain good security decisions independently—building internal judgement and expertise rather than permanent consultancy dependency. Sustainable security requires more than governance structures and technical controls—it requires people who understand security, care about it, and have the skills to implement it effectively.

Awareness Programme Design

Security awareness programme design and delivery tailored to organisational context

Executive Briefings

Executive security briefings for boards and senior leadership teams

Capability Assessments

Security capability assessments and training needs analysis

Team Coaching

Security team coaching and mentoring to build internal expertise

Our approach recognises that security awareness training alone does not change behaviour. Effective security culture requires visible leadership commitment, integration of security into performance management, practical guidance that helps people do their jobs securely, and consequences that reinforce security expectations.

Engagement Models

E2E SC offers flexible engagement models to match different organisational needs, from short-term advisory projects to long-term embedded support arrangements. All engagements are scoped to deliver defined outcomes rather than simply providing consultant time.

Advisory Projects

Fixed-scope engagements delivering specific outcomes, 4 weeks to 6 months duration

Embedded Support

Ongoing consultant placement within client organisations, monthly retainers with defined service levels

Managed GRC Services

Outsourced operation of security governance functions with regular reporting

Transformation Programmes

Comprehensive engagements combining multiple capabilities, 12-24 months duration

Service Pricing

E2E SC services are priced based on consultant day rates varying by seniority and expertise. Project pricing is calculated based on estimated effort with fixed-price options available for well-defined scopes. All prices exclude VAT and expenses.

Consultant Day Rates

Role	Day Rate
Principal Consultant / Practice Lead	**£1,200**
Senior Consultant	**£950**
Consultant	**£750**
Associate Consultant	**£550**

Indicative Project Pricing

- Security Governance Framework Design: £15,000 - £35,000
- Security Risk Assessment (organisation-wide): £20,000 - £45,000
- ISO 27001 Gap Analysis and Roadmap: £12,000 - £25,000
- Cyber Essentials Plus Certification Support: £5,000 - £12,000
- Security Strategy Development: £18,000 - £40,000
- CAF Self-Assessment Support: £15,000 - £30,000

Embedded support and managed services are priced on a monthly retainer basis, typically ranging from £8,000 to £25,000 per month depending on scope and service levels. Transformation programmes are individually scoped and priced based on detailed requirements analysis.

Service Delivery Approach

E2E SC's service delivery is structured around proven methodologies aligned with ISO 9001 quality management and ISO 27001 information security standards, supported by ITIL-aligned service management processes.

Engagement Governance

Every engagement is assigned a dedicated Account Manager responsible for overall relationship management and service quality, with Service Delivery Managers for operational coordination.

Quality Assurance

All deliverables undergo quality review before client submission, with senior consultants ensuring consistency with E2E SC standards and client requirements.

Knowledge Transfer

We design engagements to build client capability rather than create permanent consultancy dependence, including training, documentation, and coaching.

Continuous Improvement

Client feedback is systematically collected and acted upon, with post-engagement reviews capturing lessons learned and improvement opportunities.

Regular service reviews assess delivery quality, progress against objectives, and emerging requirements. For embedded and managed service engagements, monthly service reviews with client stakeholders ensure alignment between service delivery and organisational priorities.

Team and Expertise

E2E SC consultants combine deep technical expertise with practical experience implementing security governance in complex organisations. Our team includes professionals with backgrounds in central government, critical national infrastructure, financial services, healthcare, and defence sectors.

Professional Qualifications

CISSP, CISM, CRISC, ISO 27001 Lead Auditor, NCSC Certified Cyber Professional, and sector-specific qualifications

Security Clearances

All staff undergo BS7858:2019 background screening, with clearances up to Developed Vetting (DV) level for sensitive work

Sector Experience

Central government, local authorities, NHS, police, defence, CNI, and regulated financial services

Continuous Development

Ongoing professional development ensures our team remains current with evolving threats, technologies, and regulatory requirements

Support Model

E2E SC provides comprehensive support for all advisory engagements, ensuring clients receive responsive assistance throughout the engagement lifecycle and beyond.

Service Desk

Our Service Desk operates 24/7/365 as the primary point of contact for all service requests, incidents, and escalations. Each query is triaged immediately, and a ticket number is issued with an initial response within 15 minutes.

Response and Resolution Times

Priority	Description	Response	Resolution
P1	Critical: Engagement blocked, urgent client need	15 minutes	4 hours
P2	High: Significant impact on delivery or quality	1 hour	8 hours
P3	Medium: Delivery impacted, workarounds available	4 hours	2 working days
P4	Low: Minor issues, questions, or enhancements	1 working day	5 working days

Following engagement completion, clients can access ongoing advisory support through retained hours arrangements or ad-hoc requests. This ensures continuity of expertise as governance frameworks evolve and new challenges emerge.

Service Benefits

Organisations engaging E2E SC for GRC advisory services achieve tangible improvements in security governance maturity, risk management effectiveness, and compliance posture.

Joined-Up Approach

Eliminates silos, enabling coordinated security across departments and functions

Market Access

Supports access to new markets through demonstrated cyber risk management capability

Loss Minimisation

Minimises financial, reputational, and customer losses from security incidents

Insurance Cost Reduction

Reduces cyber insurance costs through improved security posture and risk management

Risk-Aware Culture

Fosters a productive, risk-aware company culture that sustains security improvements

Proportionate Spending

Ensures proportionate spending through risk-based security controls and investments

Stakeholder Confidence

Enhances stakeholder confidence through independent assurance and transparency

Continuous Improvement

Provides ongoing monitoring and continuous improvement of security risks

What Makes E2E Security Consulting Different

Many consultancies can deliver governance frameworks, risk assessments, and compliance documentation. What distinguishes E2E Security Consulting is how we think about security governance—and the quality of decisions our clients can make as a result.

Judgement Over Checklists

We prioritise helping clients understand what matters, not just what frameworks require

Comfortable with Risk Acceptance

We advise where risk acceptance is appropriate, not just where remediation is needed

Governance Under Scrutiny

We design governance that works after incidents, during audits, and in front of boards

High-Accountability Environments

We regularly advise clients where decisions have real consequences

Post-Incident Examination

We understand how decisions are examined after incidents and help clients prepare

Clarity Not Dependency

We aim to leave clients with clarity and confidence, not dependency on continued support

If you need a consultancy to produce documentation, many firms can help. If you need a consultancy to help you make decisions you can defend—to your board, your regulator, your auditors, and the public—that is what E2E Security Consulting is for.

Contact Information

For enquiries about E2E SC's GRC Advisory & Support Services, or to discuss your organisation's specific requirements, please contact us.

Email

info@e2esc.co.uk

Telephone

+44 7741 941477