Risk, Compliance & Resilience – Pricing Document

G-Cloud 15 Lot 3 Cloud Support

January 2026 – v3.0

Introduction

IVARTY Consulting Ltd, established in 2017 and registered in Scotland (SC579411), provides specialist cyber security, risk management, and resilience advisory services aligned to the Skills Framework for the Information Age (SFIA). This pricing document sets out transparent, SFIA-aligned day rates for Risk, Compliance & Resilience advisory services delivered under CCS G-Cloud 15 Framework, Lot 3 – Cloud Support.

The company operates a director-led boutique advisory model ensuring senior practitioner involvement in all engagements. Steve Metcalfe (co-director) provides cloud security architecture and technical security expertise including AWS certification and hands-on cloud security experience across Scottish and UK public sector. Mary McLuskey MBA (co-director) provides strategic transformation leadership, programme oversight, and stakeholder management ensuring security initiatives deliver measurable business value. This director-led approach provides customers with senior expertise at mid-tier pricing without large consultancy overheads.

IVARTY delivers measurable social value through remote-first operations avoiding 45,000 miles and 12 tCO2e annually, charitable partnerships providing £12,000+ to Down's Syndrome Scotland and Oor Club since 2019, comprehensive EDI commitments ensuring minimum 20% delivery hours by underrepresented groups (women in technical roles, ethnic minorities, LGBTQ+ individuals, disabled persons), and skills development focus including 5% workforce from disadvantaged backgrounds, 2 apprenticeships/graduate placements annually, and pro bono mentoring for individuals entering security sector. Service-specific social value includes documented security improvement roadmaps enabling evidence-based investment decisions, free security posture assessments for Scottish public sector SMEs (annual value £4,500), annual security seminar providing free CPD (120+ attendees 2024), and security awareness training included in all engagements at no additional charge.

Service Coverage

The Risk, Compliance & Resilience service encompasses seven core service pillars addressing cyber security, compliance, risk management, and organisational resilience. Detailed service descriptions are provided in the Service Definition v3.0. Service pillars include:

Cyber Security Assessment and Posture Improvement

Independent evaluation against NIST Cybersecurity Framework, ISO 27001:2022, CIS Controls v8, NCSC Cyber Assessment Framework, and Cyber Essentials Plus including baseline assessment, gap analysis, threat landscape evaluation, vulnerability assessment, and penetration testing where scoped.

Compliance Framework Implementation

Support for ISO 27001, ISO 27017/27018, PCI DSS, UK GDPR, NHS DSPT, and HMG Security Policy Framework including framework selection, gap analysis, policy development, implementation roadmaps, and internal audit support.

Risk Management and Governance

Risk management framework development, information security risk assessment, third-party risk assessment, cloud adoption risk assessment, governance structure design, and security metrics development.

Business Continuity and Disaster Recovery Planning

Business impact analysis, business continuity planning, disaster recovery planning, backup and restoration procedures, cloud DR strategies, and DR testing exercises.

Security Architecture and Design Review

Security architecture frameworks, cloud security architecture review (AWS Well-Architected, Azure Well-Architected, CIS Benchmarks), application security design review, network security architecture, zero trust guidance, and secure cloud migration architecture.

Incident Response Planning and Readiness

Incident response plan development, readiness assessment, tabletop exercises, UK GDPR breach notification procedures, and incident response team training.

Security Awareness and Capability Development

Security awareness programmes, phishing simulation, security champions networks, specialist training, certification roadmaps, and embedded knowledge transfer.

Quality assurance is provided through director QA oversight before customer submission and independent peer review by Lead Security Architect or external security practitioners ensuring consistency across assessments, accuracy of risk ratings, and alignment to recognised frameworks.

Pricing covers advisory assessment and design only and does not include continuous monitoring, managed security services, or operational assurance.

SFIA-Aligned Roles and Day Rates

All resources are aligned to SFIA levels 4 to 7 based on autonomy, influence, complexity, and business skills. Day rates reflect SFIA level, market rates, and expertise required. Resources at the same SFIA level are charged at the same rate regardless of sourcing (core team, Brightwork partnership, or trusted associates).

Role	SFIA Level	Day Rate	Typical Activities
Consulting Director / Partner	7	**£975 per day**	Strategic oversight of cyber security programmes, quality assurance of security assessments and architecture recommendations, senior stakeholder engagement with CISOs and governance boards, independent peer review of technical deliverables, framework governance
Chief Information Security Officer (vCISO)	7	**£975 per day**	Virtual CISO services providing strategic advisory security leadership, security policy and governance framework development, board reporting on security posture and risk, regulatory compliance oversight, security transformation programme leadership
Lead Security Architect	6	**£850 per day**	Security architecture framework development, cloud security architecture review (AWS Well-Architected, Azure, multi-cloud), zero trust architecture guidance, security design patterns, technical mentoring of customer security teams
Delivery Lead	6	**£750 per day**	Day-to-day engagement coordination, customer liaison as single point of contact, progress tracking and reporting, issue identification and escalation, resource coordination across security specialists
Business Engagement Manager	6	**£750 per day**	Stakeholder management and alignment of security objectives with organisational goals, business case development for security investments, facilitation of stakeholder workshops, change management guidance
Cyber Security Consultant / GRC Consultant	5-6	£700 per day	Security posture assessments (NIST, ISO 27001, CIS, NCSC CAF), gap analysis and remediation planning, compliance framework implementation, risk assessment and management, policy development, incident response planning
Penetration Tester / Security Analyst	5	£700 per day	Vulnerability scanning and assessment, penetration testing (CREST-aligned methodologies), security configuration review, threat intelligence research, security incident analysis

Director-level QA oversight and independent peer review are included in all security assessment and architecture deliverables at no additional charge, ensuring consistent quality and objectivity. All resources undergo appropriate security vetting (BPSS, SC, or DV) as required for customer environment with vetting costs included in day rates.

Specialist IVARTY Consulting role titles are mapped to the closest equivalent Digital Marketplace roles for pricing purposes, based on SFIA level and responsibility.

Cost Calculation Example

The following example illustrates typical engagement costs based on a real customer engagement (Scottish Local Authority Cyber Security Assessment detailed in Case Study 1 of the Service Definition v3.0):

Engagement: Comprehensive cyber security assessment using NCSC Cyber Assessment Framework (CAF) and CIS Controls v8 including baseline security posture evaluation, gap analysis, vulnerability scanning, stakeholder interviews, phishing simulation, security improvement roadmap, and Cyber Essentials Plus readiness assessment.

Resource Allocation:

Consulting Director / Partner: 3 days × £975 = **£2,925**
(QA review of assessment findings, stakeholder briefings with audit committee and senior leadership, approval of final recommendations)

Lead Security Architect: 4 days × £850 = **£3,400**
(Technical oversight of vulnerability assessment, architecture review of Azure environment, zero trust roadmap development)

Cyber Security Consultant: 10 days × £700 = **£7,000**
(CAF assessment against 14 objectives, stakeholder interviews, evidence collection, gap analysis, remediation roadmap development)

Penetration Tester: 3 days × £700 = **£2,100**
(External vulnerability scanning, phishing simulation campaign targeting 150 staff, findings analysis)

£15,425

Total Engagement Cost

20 days

Volume discount (5% for 21-40 days): Not applicable (engagement under 21 days)

Outcomes Delivered: CAF baseline assessment with overall CAF-A (foundation) rating across 14 objectives, security improvement roadmap approved by audit committee with £180K budget allocation, quick wins delivered within 6 months including MFA rollout to privileged accounts and vulnerability remediation, Cyber Essentials Plus certification achieved within 9 months enabling £4.2M framework contract bids, and annual security posture review commissioned for ongoing improvement tracking.

Commercial Terms and Ordering

Expenses

All day rates are inclusive of standard delivery costs including remote delivery infrastructure (video conferencing, secure file transfer, collaboration tools), preparation time and pre-engagement research, documentation and deliverable production, and internal quality assurance review. Remote-first delivery is standard operating model with customer site visits only where required for physical security assessment, stakeholder workshops requiring face-to-face engagement, or customer preference. Travel, subsistence, and accommodation expenses for customer-required on-site attendance are included in day rates at no additional charge, reinforcing environmental sustainability commitments through minimised business travel.

Volume Discounts

Volume discounts apply automatically to engagements exceeding 20 person-days total effort calculated across all resources and roles:

21-40 person-days total

5% discount applied to total engagement cost

41+ person-days total

10% discount applied to total engagement cost

Repeat engagement discount

Customers commissioning follow-on engagements within 12 months receive additional **3% loyalty discount** on top of volume discounts where applicable

This supports ongoing security improvement programmes with annual security posture reviews, periodic penetration testing, or phased compliance framework implementation over multiple years.

Volume discounts are calculated on total person-days for the engagement as specified in the Statement of Work and applied to the final invoice. Discounts are cumulative where both volume and loyalty discounts apply, providing maximum value for sustained security advisory relationships.

Fixed-Price Option

Fixed-price engagements are available for well-defined scopes with clear deliverables and acceptance criteria. Fixed pricing is based on estimated effort using SFIA day rates with contingency for reasonable scope variation, providing cost certainty for budget planning while maintaining delivery flexibility for emerging requirements within agreed scope boundaries.

Common fixed-price engagement types include:

- **Cyber Essentials Plus gap analysis and certification readiness assessment:** Comprehensive assessment against five technical controls (firewalls, secure configuration, user access control, malware protection, patch management), remediation guidance, internal readiness validation, and liaison with certification body. Typical fixed price **£6,500 to £9,500** depending on organisation size (under 250 users to over 1,000 users) and IT estate complexity.
- **NCSC Cyber Assessment Framework (CAF) baseline assessment:** Assessment against 14 CAF objectives with evidence-based scoring, gap analysis, and remediation roadmap. Typical fixed price **£12,000 to £18,000** depending on organisation size and number of in-scope systems.
- **ISO 27001:2022 gap analysis:** Assessment against 93 Annex A controls, ISMS scope definition, risk assessment workshop, Statement of Applicability development, and implementation roadmap. Typical fixed price **£15,000 to £25,000** depending on ISMS scope and organisational complexity.
- **Incident response plan development:** Documented incident response procedures, GDPR breach notification playbook, incident classification schema, response team structure, and tabletop exercise. Typical fixed price **£8,000 to £12,000** depending on organisation size and integration requirements with existing processes.
- **Security architecture review for cloud migration:** Assessment of proposed cloud architecture against AWS Well-Architected Security Pillar or Azure Well-Architected Framework, threat modelling, security design recommendations, and landing zone security baseline. Typical fixed price **£10,000 to £18,000** depending on workload complexity and multi-cloud requirements.

Fixed-price scopes are confirmed in Statement of Work with deliverable acceptance criteria, timescales, dependencies, and assumptions. Scope changes outside agreed boundaries are managed through change control process with commercial impact assessment before approval. Fixed-price engagements provide budget certainty while maintaining quality through director oversight and independent peer review included as standard.

What's Not Included

This advisory service does not include managed security operations (SOC/NOC monitoring, 24/7 threat detection, security event triage), security implementation (firewall configuration, endpoint deployment, SIEM installation, DLP tuning, network infrastructure changes), standalone penetration testing (penetration testing is only provided as part of broader security assessment engagements, not as isolated technical testing service), certification body services for ISO 27001, Cyber Essentials, or other formal certifications requiring UKAS or equivalent accreditation (IVARTY provides gap analysis and readiness assessment but not formal certification audits), software development or application remediation (vulnerability identification and remediation guidance provided but not code development or application modification), or GRC platform procurement or configuration (tool selection advisory provided but not license procurement or platform implementation).

Buyers requiring implementation support, managed security services, or formal certification should engage separate suppliers with appropriate capabilities and accreditations. IVARTY can provide recommendations for implementation partners, managed service providers, or certification bodies based on knowledge of market capabilities and customer requirements while maintaining advisory independence.

Delivery Assumptions and Ordering Information

Delivery Assumptions

Pricing assumes the following delivery model and customer obligations:

Remote delivery is the default operating model using Microsoft Teams, Zoom, or customer-preferred video conferencing with secure file transfer via encrypted channels. On-site delivery is provided where required for physical security assessments, stakeholder workshops requiring face-to-face engagement, or customer preference with travel costs included in day rates.

Customer access to personnel for interviews and workshops (security teams, IT operations, business process owners, senior leadership), systems and data required for security assessments (configuration exports from Active Directory, Azure AD, AWS IAM, firewall rulesets, vulnerability scan results where available, log samples, security policies and procedures), documentation (architecture diagrams, network maps, data flow diagrams, risk registers, previous audit reports), and premises for site visits where physical security assessment is required (data centres, server rooms, backup storage locations). Network access for vulnerability scanning or penetration testing requires customer-managed firewall rule changes, scanning windows agreed with operations teams, and change control approvals.

Security vetting processed according to customer requirements with typical timescales of 4-6 weeks for Baseline Personnel Security Standard (BPSS), 8-12 weeks for Security Check (SC), and 18-26 weeks for Developed Vetting (DV). Vetting costs are included in day rates. Security vetting requirements are confirmed during discovery stage and factored into engagement mobilisation planning.

Resource mobilisation typically commences within 10 working days of Statement of Work signature for standard engagements not requiring security clearance, with additional lead time for clearance processing where required. Assessor capacity is managed through advance booking with peak periods September-November (financial year-end audit preparation) and January-March (year-end compliance cycles) potentially requiring longer mobilisation lead times. Early engagement with IVARTY during budget planning cycles enables resource reservation for planned security initiatives.

Ordering Information

To order Risk, Compliance & Resilience advisory services:

01

Contact IVARTY

Contact IVARTY Consulting Ltd via email (steve@ivartyconsulting.com) or through CCS Digital Marketplace messaging with outline requirements including organisation context, security or compliance objectives, preferred timescales, and any specific framework or regulatory requirements (ISO 27001, Cyber Essentials Plus, NCSC CAF, UK GDPR).

02

Initial Scope Assessment

IVARTY conducts initial scope assessment at no cost to understand requirements, confirm service suitability, and identify appropriate resources and SFIA levels. This typically involves 30-60 minute discovery call with key stakeholders followed by review of any relevant existing documentation such as previous security assessments, compliance certifications, or strategic plans.

03

Statement of Work Development

Statement of Work (SoW) is developed specifying resources and SFIA levels with named consultants where known, person-days allocated by role and activity, deliverables with acceptance criteria and formats, timeframes with key milestones and dependencies, total cost including any applicable volume or loyalty discounts, payment terms (typically monthly arrears for time and materials or milestone-based for fixed-price), assumptions and dependencies, and change control process for managing scope variations.

04

Digital Marketplace Call-Off

Digital Marketplace call-off process is initiated with SoW attached to call-off contract. CCS processes call-off with IVARTY engagement commencing upon call-off approval and SoW signature, typically within 5 working days of call-off completion. There is no minimum engagement value - IVARTY supports engagements from single-day security advisory sessions through to multi-month compliance transformation programmes.

05

Resource Confirmation

Resource availability is confirmed before Statement of Work signature ensuring committed resources are available for agreed timescales. Where specific individual expertise is required (e.g., AWS-certified security architect for cloud migration security review), named resources are confirmed in SoW with contingency arrangements documented for unforeseen availability changes.

Framework Alignment and Document Precedence

This Pricing Document should be read in conjunction with the Risk, Compliance & Resilience Service Definition v3.0 which provides detailed service scope, delivery approach, engagement process, quality assurance, evidence of capability, and technical methodologies. Together these documents provide complete commercial and technical specification for Risk, Compliance & Resilience advisory services.

In the event of conflict between contract documents, the order of precedence is: G-Cloud 15 Framework Agreement (governs overall supplier-customer relationship and CCS obligations), Call-Off Contract (governs specific engagement terms and conditions), Statement of Work (takes precedence for engagement-specific scope, deliverables, timescales, and resource allocation), Pricing Document (governs commercial terms, day rates, discounts, and payment mechanisms), Service Definition (governs service scope, capabilities, methodologies, and quality standards). This hierarchy ensures clarity in contract interpretation and dispute resolution while enabling engagement-specific customisation through Statements of Work.

IVARTY operates rigorous alignment processes ensuring all customer-facing documentation including Statements of Work, deliverable specifications, and progress reports aligns to committed Service Definition scope, Pricing Document commercial terms, and contractual obligations. Internal quality assurance reviews verify contract alignment before customer submission. Where conflicts or ambiguities are identified during engagement delivery, these are escalated immediately through established governance mechanisms for resolution via change control process documented in Statement of Work.

Contact Information

IVARTY Consulting Ltd
15 Paterson Way, Cambusbarron
Stirling FK7 9RF, UK

Email: steve@ivartyconsulting.com
Digital Marketplace: IVARTY Consulting Ltd

Company Registration: SC579411
VAT Number: 481446578
ICO Registration: ZA796363
Established: 2017

Document Version: v3.0 – January 2026
Aligned to: Service Definition v3.0
Status: Final