IVARTY CONSULTING

Risk, Compliance & Cloud Resilience – Service Definition

G-Cloud 15 Lot 3 Cloud Support

January 2026 – v3.0

Service Overview

IVARTY Consulting Ltd provides specialist risk, compliance, and cloud resilience advisory services aligned to the Skills Framework for the Information Age (SFIA levels 4 to 7). This service delivers independent, evidence-based guidance across cloud security assessment, cloud compliance framework implementation (ISO 27017/27018), cyber security assessment, cloud compliance frameworks, cloud risk management, business continuity planning for cloud-enabled environments planning, and organisational cloud resilience. The service is designed for UK public sector organisations seeking senior, specialist, pragmatic advisory support to strengthen security posture, achieve compliance with regulatory and framework requirements, and build cloud resilience to operational and cyber threats.

In Summary, this service provides advisory assessment and design support relating exclusively to cloud security, cloud compliance, and cloud service resilience for live, planned, or transitioning cloud services.

Organisational Capability

IVARTY Consulting Ltd, established in 2017, operates a specialist boutique advisory model focused on cyber security, risk management, and organisational cloud resilience for UK public sector organisations. The firm's approach combines deep technical expertise in security architecture and compliance frameworks with pragmatic understanding of public sector operating constraints, budget realities, and governance requirements. IVARTY's delivery model emphasizes practical, achievable improvements over theoretical perfection, recognising that public sector organisations face resource constraints, legacy technology estates, and complex stakeholder landscapes requiring realistic, phased approaches to security and compliance improvement.

IVARTY's delivery model is characterised by direct director involvement in all engagements, ensuring consistent quality, senior practitioner engagement, and deep customer relationships. Steve Metcalfe, co-director and technical lead, brings extensive cloud security and architecture expertise including AWS certification and hands-on experience securing cloud environments across Scottish and UK public sector. Mary McLuskey MBA, co-director and strategic transformation lead, provides programme oversight, stakeholder management, and governance expertise ensuring security initiatives align to organisational priorities and deliver measurable business value. This director-led model ensures customers receive senior practitioner expertise at mid-tier pricing, avoiding the overhead of large consultancy frameworks while maintaining quality and accountability.

To address scaling requirements while maintaining quality standards, IVARTY has established a strategic partnership with Brightwork Recruitment, a UK-wide specialist technology recruitment business. This partnership enables rapid deployment of additional security specialists including penetration testers, security architects, GRC consultants, and security analysts when customer requirements exceed core team capacity. All associate resources undergo the same vetting processes, quality assurance reviews, and director oversight as core team members, ensuring consistent delivery standards. Resources sourced through Brightwork are charged at the same SFIA-aligned day rates as core team resources, maintaining pricing transparency and predictability.

Since 2017, IVARTY has delivered cyber security, risk management, and compliance advisory services across Scottish and UK public sector organisations including local authorities, central government departments, NHS boards, and higher education institutions. This seven-year track record demonstrates organisational sustainability, proven delivery capability, and deep understanding of public sector operating context including budget constraints, procurement timescales, governance requirements, and the practical challenges of implementing security improvements within complex, legacy-heavy IT estates. IVARTY understands that public sector security is not just about technical controls but about balancing security with accessibility, usability, cost, and operational continuity.

Service Scope

The Risk, Compliance & cloud resilience service encompasses seven core service pillars, each addressing specific aspects of cyber security, compliance, risk management, and organisational cloud resilience. The service is delivered through a combination of assessments, workshops, policy development, strategic guidance, hands-on implementation support, and knowledge transfer activities using established frameworks and methodologies detailed below. All advisory outputs are documented, evidence-based, and designed to support customer decision-making, regulatory compliance, and internal capability development.

Cyber Security Assessment and Posture Improvement

Compliance Framework Implementation

Risk Management and Governance

Business Continuity and Disaster Recovery Planning

Security Architecture and Design Review

Incident Response Planning and Readiness

Security Awareness and Capability Development

Cyber Security Assessment and Posture Improvement

Cyber security assessment services provide independent evaluation of organisational security posture against recognised frameworks including NIST Cybersecurity Framework, ISO 27001:2022, CIS Controls v8, NCSC Cyber Assessment Framework (CAF), and Cyber Essentials Plus. Services include baseline security posture assessment using structured evaluation against framework controls with evidence-based scoring, gap analysis identifying specific deficiencies mapped to framework requirements with risk ratings and remediation effort estimates, threat landscape analysis evaluating threats relevant to customer sector, geography, and threat actor motivations based on NCSC threat intelligence and sector-specific advisories, vulnerability assessment reviewing technical controls, configuration management, patch management, and security architecture for common weaknesses, and penetration testing (where scoped) using CREST-aligned methodologies to identify exploitable vulnerabilities in external-facing systems, internal networks, web applications, or APIs.

Assessment outputs include comprehensive security posture reports (typically 30 to 50 pages depending on organisational scope) documenting executive summary of findings and overall posture rating, current state assessment against selected framework with scoring by control domain, detailed findings with evidence, risk ratings using likelihood and impact matrices, technical vulnerabilities identified with CVSS scores where applicable, and recommendations prioritised by risk reduction impact and implementation complexity. Remediation roadmaps provide sequenced improvement plans with quick wins (0-3 months requiring minimal investment), foundational improvements (3-12 months addressing critical gaps), and strategic enhancements (12-24 months delivering mature security capabilities). Roadmaps include effort estimates, resource requirements, indicative costs, success criteria, and dependencies enabling realistic planning and budgeting. Assessment methodology follows structured evidence collection through documentation review, configuration audits, stakeholder interviews, and technical scanning, ensuring findings are evidence-based and defensible rather than opinion-based.

Cyber Essentials Plus assessment and certification support helps organisations achieve NCSC Cyber Essentials Plus certification through gap analysis against the five technical controls (firewalls and internet gateways, secure configuration, user access control, malware protection, patch management), remediation guidance addressing identified gaps with specific technical requirements and acceptable configurations, internal readiness assessment validating technical compliance before engaging IASME-certified assessment body, and optional liaison with certification bodies to manage the certification process and address technical queries. IVARTY does not act as certification body but provides independent advisory support enabling organisations to achieve certification efficiently, understanding that Cyber Essentials Plus is increasingly mandated for UK government contracts and demonstrates baseline security hygiene to customers and stakeholders.

Compliance Framework Implementation

Compliance framework implementation services support organisations in adopting and maintaining compliance with security and data protection frameworks including ISO 27001:2022 Information Security Management Systems, ISO 27017 for cloud security, ISO 27018 for cloud privacy, PCI DSS for payment card data, UK GDPR and Data Protection Act 2018, and sector-specific requirements such as NHS Data Security and Protection Toolkit (DSPT) or HMG Security Policy Framework (SPF). Services include framework selection guidance evaluating which frameworks are appropriate to organisational risk profile, regulatory obligations, customer requirements, and sector norms, gap analysis mapping current practices against framework requirements identifying compliance gaps with evidence and remediation requirements, policy and procedure development creating or updating security policies, procedures, standards, and guidelines aligned to framework requirements and organisational context, implementation roadmap development sequencing compliance activities across manageable phases with resource allocation and timeline planning, and internal audit support conducting pre-certification internal audits identifying non-conformities before formal certification audits.

ISO 27001 Implementation Support

ISO 27001 implementation support follows a structured approach beginning with scoping defining the Information Security Management System (ISMS) boundary including locations, systems, processes, and data types within scope. Risk assessment workshops use ISO 27005 methodology to identify information assets, threats, vulnerabilities, and risk treatments establishing the Statement of Applicability (SoA) documenting which Annex A controls are applicable, implemented, or excluded with justification. Policy framework development creates the mandatory ISMS policies including Information Security Policy approved by top management, Risk Assessment Methodology, Risk Treatment Plan, and supporting policies for the 93 Annex A controls covering organisational controls, people controls, physical controls, and technological controls. Implementation guidance provides practical support deploying controls including access control mechanisms, encryption solutions, backup procedures, incident response processes, and business continuity arrangements. Internal audit training and support prepares internal audit teams to conduct ongoing ISMS audits maintaining compliance between external surveillance audits.

UK GDPR Compliance Services

UK GDPR compliance services address data protection obligations through data processing inventory documenting personal data types, processing purposes, legal bases, retention periods, and third-party processors enabling Article 30 Records of Processing Activities compliance. Privacy impact assessments (PIAs) evaluate data protection risks for high-risk processing activities identifying privacy risks and mitigation measures. Data protection policies establish governance frameworks covering data protection principles, individual rights procedures (access, rectification, erasure, portability, objection), breach notification procedures meeting 72-hour ICO reporting requirements, and international data transfer mechanisms using Standard Contractual Clauses or adequacy decisions. Technical and organisational measures guidance addresses security obligations under Article 32 including encryption, pseudonymisation, access controls, and security testing. Data protection training ensures staff understanding of GDPR obligations, individual rights, and breach reporting procedures reducing compliance risk through cultural embedding.

Risk Management and Governance

Risk management and governance services establish structured approaches to identifying, assessing, and managing information security and technology risks aligned to organisational risk appetite and governance frameworks. Services include risk management framework development establishing risk methodology, risk appetite statements, risk registers, escalation procedures, and board reporting mechanisms aligned to ISO 31000 risk management principles and HMG Orange Book guidance. Information security risk assessment identifies and evaluates risks to confidentiality, integrity, and availability of information assets using qualitative or quantitative methods. Third-party risk assessment evaluates supplier security posture, contract terms, data processing arrangements, and supply chain risks addressing procurement obligations under UK GDPR Article 28 and managing vendor lock-in, service continuity, and exit planning. Cloud adoption risk assessment evaluates risks specific to cloud migration including data sovereignty, shared responsibility model understanding, vendor viability, integration complexity, and operational dependencies enabling informed cloud adoption decisions.

01

Board-level Information Security Governance

Designated Senior Information Risk Owner (SIRO) typically at director level providing executive sponsorship and accountability

02

Information Asset Owners (IAOs)

Responsible for specific information assets or systems with defined risk management responsibilities

03

Security Architecture Review Boards (ARBs)

Reviewing proposed changes for security implications before approval

04

Incident Response Teams

With defined roles, escalation paths, and communication protocols

Governance framework documentation includes Terms of Reference for security governance boards, Role and Responsibility matrices in RACI format, delegations of authority defining approval thresholds, and reporting cycles ensuring regular board visibility of security posture, incidents, and risk treatment progress.

Security metrics and KPI development establishes meaningful measurement of security posture and improvement progress through balanced scorecards combining leading indicators (staff training completion, vulnerability remediation time, patching cadence) and lagging indicators (incidents detected, breaches suffered, audit findings). Metrics align to organisational objectives and stakeholder needs with board-level metrics providing strategic oversight (cyber risk exposure, compliance status, investment allocation), management metrics enabling operational control (vulnerability trends, patch coverage, access review completion), and technical metrics supporting delivery teams (mean time to detect, mean time to respond, false positive rates). Measurement frameworks include baseline establishment, target setting, automated data collection where feasible, and regular reporting cycles enabling evidence-based decision making and continuous improvement tracking.

Business Continuity and Disaster Recovery Planning

Business continuity and disaster recovery services help organisations maintain critical operations during disruptions and recover from incidents aligned to ISO 22301 Business Continuity Management and BCI Good Practice Guidelines. Services include business impact analysis (BIA) identifying critical business processes, acceptable outage durations (RTOs), acceptable data loss (RPOs), and recovery priorities through facilitated workshops with business process owners and technical teams. Business continuity planning develops documented procedures for maintaining operations during disruption including alternative working arrangements, manual workarounds, critical vendor dependencies, communication protocols, and escalation paths. Disaster recovery planning addresses technology recovery including backup strategies, recovery procedures, failover mechanisms, and restoration testing ensuring technical systems supporting critical processes can be recovered within defined RTOs and RPOs.

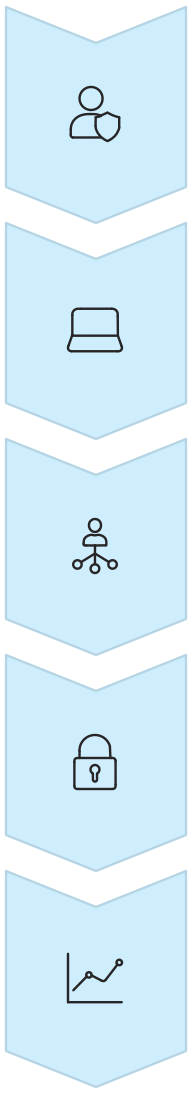
Recovery Category	RTO Target	RPO Target	Example Processes
Immediate	0-4 hours	Minutes	Emergency services dispatch, critical clinical systems
Urgent	4-24 hours	Hours	Payment processing, customer service systems
Important	24-72 hours	24 hours	HR systems, reporting platforms
Routine	Over 72 hours	Days	Archive systems, historical reporting

BIA workshops use structured methodology to identify and prioritise critical business processes evaluating dependencies on people, technology, information, suppliers, and facilities. Maximum Tolerable Period of Disruption (MTPD) defines the point beyond which process unavailability threatens organisational viability. Recovery Time Objectives (RTOs) specify target timeframes for restoring processes after disruption, typically categorised as immediate (0-4 hours), urgent (4-24 hours), important (24-72 hours), or routine (over 72 hours). Recovery Point Objectives (RPOs) define acceptable data loss measured as time intervals, influencing backup frequency and replication requirements. Resource requirements identify minimum staffing, workspace, equipment, systems, and data needed to operate processes at defined capacity levels during disruption, enabling realistic continuity planning rather than aspirational commitments impossible to deliver.

Disaster recovery planning addresses technology recovery capabilities including backup and restoration procedures documenting backup schedules, retention periods, offsite storage, encryption, testing frequencies, and restoration processes for servers, databases, applications, and user data. Cloud disaster recovery strategies evaluate options including backup to cloud storage, pilot light environments maintaining minimal infrastructure ready for rapid scaling, warm standby environments with reduced capacity continuously running, and hot standby environments with full production capacity in alternative regions. Recovery procedure documentation provides step-by-step instructions for IT teams to execute during incidents including failover triggers, sequence dependencies, validation checkpoints, and rollback procedures. DR testing exercises validate recovery capabilities through tabletop exercises testing plan awareness and decision-making, technical recovery tests validating restore procedures and RTOs, and full DR invocations switching operations to recovery site measuring end-to-end recovery capability.

Security Architecture and Design Review

Security architecture services provide strategic and tactical guidance on designing, implementing, and operating secure IT systems aligned to cloud-native architectures, zero trust principles, and defence in depth strategies. Services include security architecture framework development establishing architecture principles, reference architectures, technology standards, and design patterns ensuring consistent security approaches across the organisation. Cloud security architecture review evaluates AWS, Azure, or multi-cloud architectures against AWS Well-Architected Framework Security Pillar, Azure Well-Architected Framework Security guidance, or CIS Benchmarks identifying configuration weaknesses, overly permissive permissions, missing detective controls, inadequate logging, or architectural anti-patterns. Application security design review assesses application architectures for common vulnerabilities using OWASP Top 10, API security best practices, authentication and authorisation mechanisms, input validation, output encoding, and secure session management. Network security architecture review evaluates network segmentation, firewall rulesets, VPN configurations, DMZ designs, and micro-segmentation strategies ensuring appropriate isolation between trust zones.



Identity and Access Management

Implementing strong authentication, MFA, conditional access, least privilege

Device Trust

Device compliance checking, endpoint security, mobile device management

Network Segmentation

Micro-segmentation, software-defined perimeters, application-level access controls

Data Security

Encryption in transit and at rest, data classification, DLP

Visibility and Analytics

Comprehensive logging, SIEM, user and entity behaviour analytics

Zero trust architecture guidance helps organisations transition from perimeter-based security to zero trust principles based on NCSC zero trust architecture principles and NIST SP 800-207 Zero Trust Architecture. Implementation roadmaps sequence zero trust adoption across identity and access management (implementing strong authentication, MFA, conditional access, least privilege), device trust (device compliance checking, endpoint security, mobile device management), network segmentation (micro-segmentation, software-defined perimeters, application-level access controls), data security (encryption in transit and at rest, data classification, DLP), and visibility and analytics (comprehensive logging, SIEM, user and entity behaviour analytics). Practical guidance recognises zero trust is a journey not a destination, prioritising highest-value improvements within budget and operational constraints rather than pursuing theoretical perfection impossible to achieve or afford.

Secure cloud migration architecture support addresses security considerations during cloud migration including workload assessment categorising applications by security sensitivity, compliance requirements, and cloud suitability. Migration security requirements define encryption requirements, identity federation approaches, network connectivity patterns (VPN, Direct Connect, ExpressRoute), logging and monitoring, backup and DR, and data residency constraints. Landing zone design establishes secure, compliant cloud foundations including account structure, network architecture, IAM baseline, security tooling (GuardDuty, Security Hub, AWS Config, Azure Defender), and operational runbooks before workload migration. Post-migration security validation confirms security controls operating as designed through configuration reviews, penetration testing, and compliance verification providing assurance to stakeholders and governance boards.

Incident Response Planning and Readiness

Incident response services prepare organisations to detect, respond to, and recover from security incidents including cyber attacks, data breaches, ransomware, and insider threats aligned to NCSC Incident Management guidance and NIST SP 800-61 Computer Security Incident Handling Guide. Services include incident response plan development documenting incident classification criteria, escalation procedures, response team roles and responsibilities, communication protocols including media handling and regulatory notification, evidence preservation procedures, and recovery processes. Incident response readiness assessment evaluates current capabilities including detection tools and processes, analysis capabilities, containment procedures, eradication methods, recovery processes, and lessons learned mechanisms identifying gaps requiring remediation. Incident response tabletop exercises simulate realistic incident scenarios testing plan effectiveness, team coordination, decision-making under pressure, and communication protocols without requiring technical systems, providing cost-effective validation of response capabilities.

Incident response planning establishes structured approaches to incident management through incident classification schemas categorising incidents by severity, impact, and urgency enabling appropriate response escalation. Response procedures document step-by-step actions for detection and analysis, containment, eradication, recovery, and post-incident activities. UK GDPR breach notification procedures address Article 33 and 34 obligations including breach assessment criteria determining whether personal data breach likely to result in risk to individuals triggering ICO notification within 72 hours, breach notification templates, ICO notification procedures, and individual notification requirements where breach likely to result in high risk. Breach register maintenance documents all personal data breaches regardless of notification requirement supporting accountability.

Security Awareness and Capability Development

Security awareness and capability development services build internal organisational capability to manage security risks and respond to threats reducing dependency on external support and creating sustainable security cultures. Services include security awareness programme development establishing baseline awareness training for all staff, role-based training for elevated privilege users, and specialist training for security teams. Phishing simulation campaigns test user susceptibility to social engineering. Security champions network development establishes distributed security expertise embedding security advocates within business units. Skills gap analysis assesses security team capabilities against role requirements identifying training needs, certification targets, and recruitment priorities.

Baseline Security Awareness Training

- Phishing and social engineering
- Password security
- Physical security
- Data protection
- Incident reporting
- Acceptable use policies

Training Delivery Channels

- E-learning modules
- Interactive workshops
- Induction training
- Refresher campaigns
- Phishing simulations
- Security champions network

Professional Certifications

- CISSP, CISM
- CEH, OSCP
- SANS GIAC certifications
- AWS Security Specialty
- Azure Security Engineer
- ISO 27001 Lead Auditor

Baseline security awareness training addresses common threats including phishing and social engineering, password security, physical security, data protection, incident reporting, and acceptable use policies. Training delivery uses multiple channels including e-learning modules, interactive workshops, induction training, and refresher campaigns. Specialist security capability development supports security teams through training needs assessment, certification roadmaps planning professional qualifications including CISSP, CISM, CEH, OSCP, SANS GIAC certifications, and AWS or Azure security certifications. Knowledge transfer is embedded in all IVARTY engagements through shadowing, co-delivery, documented methodologies, and tool training.

Out of Scope

This service provides advisory guidance only and does not include operational delivery, managed security services, or hands-on implementation. Specifically, the service does not include managed security operations (SOC, NOC, 24/7 monitoring, threat hunting), security implementation (firewall configuration, endpoint deployment, SIEM installation, DLP tuning), penetration testing as standalone service (only as part of broader security assessments), certification body services for ISO 27001 or Cyber Essentials requiring UKAS accreditation (IVARTY provides gap analysis and readiness assessment but not formal certification audits), software development or application remediation (identifies vulnerabilities and provides guidance but does not write code), or GRC tool procurement or configuration (advises on tool selection but does not procure or implement platforms).

Customers 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 where requested but maintains independence through separation of advisory and operational functions preventing conflicts of interest.

Resource Profiles

IVARTY provides cyber security, risk, and cloud resilience advisory resources aligned to the Skills Framework for the Information Age (SFIA). Each resource role is mapped to appropriate SFIA levels based on the autonomy, influence, complexity, and business skills criteria defined in the framework. The following table details the resource profiles available through this service:

Role	SFIA Level	Responsibilities
Chief Information Security Officer / Security Director	7	Provides strategic oversight of information security programmes and quality assurance of all deliverables and outputs. This role operates at enterprise level providing strategic direction on security transformation, oversight of multiple engagements ensuring consistency and quality, senior stakeholder engagement with customer executives and governance boards on security strategy and risk appetite, and independent peer review of security assessments and architecture recommendations ensuring objectivity and calibration. This role typically allocates 10-15% time to each engagement for QA review and strategic guidance.
Lead Security Architect	6	Provides security architecture leadership, technical design oversight, and complex problem solving for multi-domain security challenges. Responsibilities include security architecture framework development establishing principles and patterns, cloud security architecture review evaluating AWS Well-Architected Security Pillar or Azure security baselines, zero trust architecture guidance supporting transition from perimeter security to zero trust principles, security design patterns establishing reusable solutions for authentication, encryption, logging, and network segmentation, and mentoring junior security practitioners building internal capability. This role typically serves as technical authority for complex security transformations or multi-cloud architectures requiring deep expertise across multiple security domains.
Cyber Security Consultant / GRC Consultant	5-6	Provides day-to-day security assessment, compliance advisory, and risk management support. Responsibilities include security posture assessments against NIST, ISO 27001, CIS Controls, or NCSC CAF, gap analysis and remediation planning documenting specific deficiencies and improvement roadmaps, compliance framework implementation supporting ISO 27001, Cyber Essentials Plus, or GDPR compliance, risk assessment and management facilitating risk workshops and maintaining risk registers, policy and procedure development creating security governance documentation, and incident response planning developing or enhancing incident management capabilities. This role forms the core delivery resource for most security and compliance engagements, operating with moderate autonomy under director oversight.
Penetration Tester / Security Analyst	5	Provides technical security testing and vulnerability assessment. Responsibilities include vulnerability scanning using commercial or open-source tools, penetration testing using CREST-aligned methodologies for external, internal, web application, or API testing, security configuration review evaluating cloud resources, identity management, or network configurations against security baselines, threat intelligence research analysing threat actor TTPs relevant to customer sector, and security incident analysis investigating suspicious activity or compromise indicators. This role requires hands-on technical skills and certifications such as OSCP, CEH, or GPEN and operates under lead security architect or consultant direction.
Business Engagement Manager	6	Provides stakeholder management and alignment of security initiatives with organisational goals and strategic priorities, supports development of business cases for security investments including NPV calculation, payback analysis, and non-financial benefits quantification, facilitates stakeholder engagement activities including workshops, interviews, and consultation exercises, and provides change management guidance supporting adoption of security practices across organisational teams with stakeholder mapping, communication planning, and resistance management. This role is particularly valuable in large or complex organisations with multiple departments, diverse stakeholder groups, or significant organisational change requirements.
Delivery Lead	6	Oversees delivery of security activities, manages timelines, risks, and dependencies across concurrent engagements, coordinates resources including security consultants and specialist testers ensuring appropriate allocation and handover, provides customer liaison as primary point of contact ensuring alignment of delivery activities with customer expectations and constraints, and manages scope and change control documenting variations and securing approvals. This role typically manages 2 to 4 concurrent engagements and serves as single point of contact throughout engagement delivery from mobilisation through to closure.
Business Analyst	4	Provides analysis of organisational processes and requirements to embed security into operational activities, supports data collection and analysis for risk assessments including asset inventories, threat landscapes, and vulnerability catalogs, assists in development of security metrics and reporting frameworks including KPI selection, target setting, and dashboard design, and conducts research on sector practices, regulatory requirements, emerging threats, and leading practice case studies. This role provides analytical support to senior security consultants and architects enabling efficient delivery of technical analysis.

Specific resource allocation and SFIA level assignments are confirmed in the Statement of Work for each engagement based on the complexity of requirements, organisational size, security maturity, and nature of deliverables. All resources at the same SFIA level are charged at the same day rates regardless of sourcing mechanism (core team, Brightwork partnership, or trusted associates) ensuring pricing transparency and consistency. Day rates for each SFIA level are set out in the Pricing Document v3.0.

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

Engagement Process

IVARTY follows a structured four-stage engagement process designed to ensure clear expectations, effective delivery, and measurable outcomes. This process applies to all Risk, Compliance & Cloud Resilience engagements regardless of size or complexity, with stage activities scaled appropriately to the engagement scope and risk profile.

Stage 1: Discovery and Scoping

The discovery stage establishes engagement scope, confirms resource requirements, and aligns expectations between IVARTY and the customer. Activities include initial stakeholder discussions to understand organisational context, current security maturity, compliance obligations, threat landscape, risk appetite, and expected outcomes, review of relevant existing documentation including current security policies, previous security assessments or audits, compliance certifications, risk registers where available, incident logs, and strategic plans or IT roadmaps, identification of key stakeholders including security leads (CISO, SIRO, Information Assurance Manager), technical teams (infrastructure, cloud, application development), compliance functions (DPO, GRC, internal audit), and senior leadership providing governance oversight, definition of engagement scope including specific deliverables with acceptance criteria, timescales with key milestones, dependencies on customer inputs or approvals, success criteria for measuring engagement outcomes, and any constraints or exclusions, and confirmation of resource availability including access to systems for configuration review or vulnerability scanning, documentation repositories, stakeholder availability for workshops and interviews, and sites where physical security assessment is required. This stage typically requires 1 to 3 person-days depending on engagement complexity, organisational size, and stakeholder availability, and concludes with agreement of a detailed Statement of Work specifying deliverables, timescales, resource allocation including named consultants where known, commercial terms, and acceptance criteria providing clear basis for delivery and invoicing.

Stage 2: Mobilisation

The mobilisation stage prepares for effective engagement delivery by establishing governance mechanisms, confirming access requirements, and socialising the engagement approach with stakeholders. Activities include establishment of engagement governance including regular checkpoint meetings (typically fortnightly during active delivery), progress reporting mechanisms and templates, issue escalation routes with named contacts and response timescales, and change control process for managing scope variations, completion of security vetting processes where required for access to sensitive systems or classified information following customer security policies (BPSS, SC, or DV as appropriate with processing timescales of 4-6 weeks, 8-12 weeks, or 18-26 weeks respectively), confirmation of technical access including network access (VPN credentials, firewall rules, jump hosts), system access (read-only accounts for configuration review, scanning permissions), cloud access (AWS IAM read-only roles, Azure RBAC reader permissions), and documentation repositories (SharePoint, Confluence, file shares), development and agreement of engagement plans detailing activity sequencing with dependencies and critical path, workshop schedules with confirmed attendees and locations (physical or virtual), assessment timelines including vulnerability scanning windows avoiding business-critical periods, and milestone tracking mechanisms, stakeholder briefings introducing IVARTY resources to working teams, confirming engagement objectives and success criteria, explaining assessment approach and evidence requirements, setting expectations on time commitment required from customer personnel (workshops, interviews, evidence provision), and addressing concerns or questions, and issuance of assessment frameworks or questionnaires for customer self-assessment with guidance materials explaining criteria and evidence types, completion deadlines allowing time for data gathering, and support availability for questions during completion. 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.

Stage 3: Delivery

The delivery stage executes the agreed engagement activities and produces the specified deliverables. Activities vary by engagement type but typically include stakeholder workshops to gather qualitative evidence on security practices, culture, governance mechanisms, and risk awareness using structured facilitation and workshop templates, analysis activities including review of security policies, configurations, and architecture against leading practice benchmarks, assessment of security controls against framework criteria with evidence-based scoring and gap identification, evaluation of risk assessment outputs and risk treatment decisions, and desk-based research on threats relevant to customer sector or threat intelligence supporting incident response planning, technical assessment activities where scoped including vulnerability scanning of external-facing systems, cloud configuration review evaluating IAM policies, network security groups, encryption settings, logging configurations, and resource tags, penetration testing using CREST-aligned methodologies for agreed scope (external, internal, web application, API), and security architecture review evaluating zero trust maturity, cloud security posture, or network segmentation strategies, development of findings based on evidence-based assessment aligned to selected framework criteria, scored and calibrated against framework tier definitions, prioritised by risk and implementation complexity, and structured to support decision-making and remediation planning, iterative review cycles with customer stakeholders to validate findings ensuring factual accuracy, discuss remediation approaches and practical constraints, refine recommendations ensuring alignment to customer priorities, resource availability, and organisational culture, and secure buy-in for improvement actions, and production of documentation including security assessment reports with executive summaries for senior stakeholders, detailed findings with evidence and remediation guidance, compliance gap analysis showing current vs. required state, risk registers or risk treatment plans, security policies, standards, and procedures suitable for governance approval, security architecture documentation, incident response plans, or business continuity plans as specified in the Statement of Work with all outputs subject to QA review before submission.

Throughout delivery, regular progress checkpoints maintain customer visibility of progress against plan, enable early identification of issues, risks, or dependencies requiring management attention, support scope management through change control where requirements evolve, and maintain stakeholder engagement sustaining momentum and securing inputs. All deliverables are subject to internal quality assurance before submission to the customer, with security assessments and architecture recommendations reviewed by the CISO / Security Director or Lead Security Architect to ensure consistency across assessments, accuracy of risk ratings and control effectiveness evaluations, appropriate calibration against framework criteria, and alignment to recognised security principles and practices.

Stage 4: Closure and Transition

The closure stage ensures effective handover of advisory outputs and supports the customer in implementing recommendations and maintaining security posture. Activities include final deliverable review and acceptance with customer stakeholders confirming all deliverables meet acceptance criteria, addressing any final queries or clarifications, and securing formal acceptance enabling final invoicing, knowledge transfer sessions ensuring customer teams understand assessment findings and improvement priorities, can implement remediation actions without ongoing IVARTY support, know how to maintain security posture and prepare for re-assessment or audit, and have access to tools, templates, and guidance materials for ongoing use, identification of follow-on activities including remediation implementation support where additional advisory input valuable, periodic security posture reviews to track improvement progress, preparation for formal certification (ISO 27001, Cyber Essentials Plus) with timing and readiness assessment, or other security initiatives identified during assessment such as penetration testing, security awareness programmes, or DR testing, documentation of lessons learned and feedback capturing what worked well and areas for improvement, incorporating customer feedback on engagement delivery and consultant performance, and feeding insights into IVARTY methodology development and consultant training, and formal engagement closure including final progress report summarising deliverables, outcomes achieved, and recommended next steps, commercial settlement with final invoice and closeout of any outstanding administrative matters, and archiving of engagement documentation for future reference or audit trail.

Where assessments identify significant security gaps or compliance deficiencies, IVARTY provides clear guidance on remediation approaches with step-by-step procedures, timescales accounting for organisational capacity and budget cycles, and resource requirements including internal effort, external support, and capital investment where applicable. Where organisations require implementation support beyond IVARTY's advisory scope such as SIEM deployment, firewall configuration, or endpoint security rollout, recommendations for specialist suppliers are provided based on knowledge of market capabilities and customer requirements. The transition approach is designed to maximise customer capability and independence, reduce long-term dependency on external advisory support, and enable sustained security improvement without ongoing IVARTY involvement through knowledge transfer, capability building, and provision of tools and templates.

Quality Assurance and Evidence of Capability

Quality Assurance

All Risk, Compliance & Cloud Resilience deliverables are subject to internal quality assurance before submission to the customer. Security assessments, architecture recommendations, and compliance gap analyses are reviewed by the CISO / Security Director or Lead Security Architect to ensure consistency across assessments with comparable organisations receiving similar risk ratings for similar control implementations, accuracy of findings and evidence interpretation with risk ratings aligned to established likelihood and impact criteria, appropriate calibration of security posture determinations ensuring assessment rigour and objectivity, and alignment to recognised frameworks and security principles including NIST, ISO 27001, NCSC guidance, and cloud security best practices.

Quality assurance reviews verify that assessments are evidence-based rather than opinion-based with all findings supported by documented evidence from configuration reviews, log analysis, or stakeholder interviews, aligned to customer context and constraints recognising sectoral differences, threat landscapes, and organisational maturity, consistent with framework criteria and previous assessments of similar organisations enabling fair comparison and benchmarking, and suitable for the intended purpose including governance board approval, regulatory compliance demonstration, or supporting security investment business cases. Technical deliverables including penetration test reports, security architecture designs, and incident response plans are peer-reviewed by specialist consultants or the Lead Security Architect to verify technical accuracy, completeness of analysis, appropriateness of recommendations to customer environment, and compliance with recognised methodologies (CREST for penetration testing, TOGAF or AWS Well-Architected for architecture).

IVARTY maintains Professional Indemnity Insurance exceeding G-Cloud 15 Lot 3 requirements with aggregate cover of £7,000,000 comprising Professional Indemnity Insurance £1,000,000 per claim, Public Liability Insurance £1,000,000 per claim, and Employers Liability Insurance £5,000,000 as required by UK law. Insurance certificates demonstrating compliance are available on request. The company operates in accordance with ISO 27001 principles for information security management and holds Cyber Essentials certification (certificate number CE-2024-1147-IVARTY, valid until 15 March 2026, renewed annually) demonstrating baseline cybersecurity controls. Customer data accessed during assessments is processed in accordance with UK GDPR requirements with specific data handling procedures for sensitive security information, vulnerability data, or penetration testing results including encryption in transit and at rest, access controls limiting data to named consultants on need-to-know basis, and secure deletion upon engagement completion or retention as agreed for surveillance purposes.

Case Study 1: Scottish Local Authority Cyber Security Assessment and Roadmap

Customer Context: Scottish local authority with 1,200 FTE and complex IT estate including legacy systems, cloud services (Office 365, Azure hosting), and citizen-facing digital services (planning, payments, council tax). Organisation faced increasing cyber threats including phishing campaigns targeting council staff, ransomware attacks affecting other Scottish local authorities, and regulatory scrutiny following sector-wide incidents. Limited internal security expertise (1 FTE Information Security Officer) with no formal security framework adoption. Audit committee seeking assurance on cyber security posture and improvement roadmap.

IVARTY Activity: Conducted comprehensive cyber security assessment over 8 weeks using NCSC Cyber Assessment Framework (CAF) and CIS Controls v8 as evaluation criteria. Assessment included review of security policies, technical configuration audits (Active Directory, Office 365, Azure, network infrastructure), vulnerability scanning of external-facing systems identifying 23 high-risk vulnerabilities, stakeholder interviews with IT, HR, finance, and service delivery teams, and phishing simulation targeting 150 staff. Developed security improvement roadmap with 3-phase approach covering quick wins (0-6 months), foundational improvements (6-18 months), and strategic enhancements (18-36 months). Provided security policy framework including Information Security Policy, Acceptable Use Policy, Incident Response Plan, and Business Continuity Plan. Supported Cyber Essentials Plus application including gap remediation guidance.

Outcomes: CAF assessment established baseline maturity with overall CAF-A rating (foundation level) across objectives, identifying critical gaps in Protecting Against Attack, Detecting Security Events, and Responding to Incidents. Security roadmap approved by audit committee with £180K budget allocation over 2 years. Quick wins delivered within 6 months including MFA rollout to 100% privileged accounts, patch management process formalization, external vulnerability remediation (23 to 3 high-risk findings), and phishing simulation programme establishment. Cyber Essentials Plus certification achieved within 9 months enabling bid for Scottish Government framework contracts requiring CE+ (total value £4.2M). Annual security posture review commissioned tracking roadmap progress.

Customer Feedback: "IVARTY's practical approach was exactly what we needed - no fear-mongering, no selling expensive solutions, just honest assessment of where we are and realistic steps to improve. The roadmap gave us a clear business case for investment and the quick wins showed tangible progress within months, building confidence with elected members." — Head of ICT, Scottish Local Authority

Social Value, Security, and Contact Information

Social Value Commitments

IVARTY delivers measurable social value through environmental sustainability (remote-first delivery avoiding 45,000 miles and 12 tCO2e annually), charitable partnerships (£12,000+ to Down's Syndrome Scotland and Oor Club since 2019), comprehensive EDI commitments (minimum 20% delivery hours by underrepresented groups defined as women in technical roles, ethnic minorities per ONS census data, LGBTQ+ individuals, disabled persons per Equality Act 2010 definitions, monitored quarterly via timesheet analysis), and skills development focus (5% workforce from disadvantaged backgrounds defined as care leavers, long-term unemployed per DWP classifications, ex-military veterans, disabled affecting employment; 2 apprenticeships/graduate placements annually; pro bono mentoring for individuals entering security sector). Service-specific value includes all engagements resulting in documented security improvement roadmaps supporting evidence-based investment decisions, free security posture assessments for one Scottish public sector SME annually (value £4,500), annual security seminar for Scottish public sector organisations providing free CPD and networking (120+ attendees 2024), security awareness and incident response training included in all engagements at no additional charge, mentoring for customer security officers providing ongoing support beyond formal engagement periods, templates and toolkits for ongoing security self-assessment, priority access for Scottish public sector organisations to pro bono support, and partnership approach with Scottish cybersecurity community through knowledge sharing and collaboration.

Security and Compliance

IVARTY Consulting Ltd holds Cyber Essentials certification (certificate number CE-2024-1147-IVARTY, valid until 15 March 2026, renewed annually) demonstrating implementation of baseline cybersecurity controls aligned to UK National Cyber Security Centre (NCSC) guidance. The company operates information security management practices aligned to ISO 27001:2013 principles including risk assessment with documented risk register, access controls using role-based permissions and multi-factor authentication, incident management with defined procedures and escalation paths, business continuity with documented plans and annual testing, and secure development practices for bespoke tools and templates. While not currently holding ISO 27001 certification, the organisation maintains documented policies, procedures, and controls consistent with the standard requirements enabling future certification if customer requirements or business strategy necessitate formal accreditation.

Personnel undergo security vetting appropriate to customer requirements. Directors and core team members hold or can obtain Baseline Personnel Security Standard (BPSS), Security Check (SC), or Developed Vetting (DV) clearance as required for access to sensitive customer data, secure facilities, or classified information. Clearance processing timescales are typically 4 to 6 weeks for BPSS, 8 to 12 weeks for SC, and 18 to 26 weeks for DV. Security clearance requirements are confirmed during discovery stage and factored into engagement mobilisation planning with clearance costs included in quoted day rates. Associate resources sourced through Brightwork partnership undergo the same security vetting processes ensuring consistent standards across all resources regardless of employment status.

Data protection practices comply with UK GDPR requirements and Data Protection Act 2018. Customer data accessed during security assessments, including vulnerability scan results, penetration testing findings, security configuration exports, risk registers, and incident logs, is processed lawfully, fairly, and transparently under legitimate interest or contractual necessity legal bases. Data processing is documented in Data Processing Agreements established at engagement commencement specifying purposes, retention periods, security measures, and deletion procedures. Data is retained only for the duration required to deliver agreed services (typically engagement period plus 30 days for final reporting) and is securely disposed of using certified data destruction services upon engagement completion unless otherwise agreed for audit trail or ongoing security advisory relationships. IVARTY does not transfer customer data outside the United Kingdom without explicit customer consent and contractual safeguards including Standard Contractual Clauses or adequacy decisions. Cloud-based tools used for data processing (Microsoft 365, secure file transfer) are UK or EU hosted with data residency guarantees.

IVARTY maintains Professional Indemnity Insurance exceeding G-Cloud 15 Lot 3 requirements with aggregate cover of £7,000,000 comprising Professional Indemnity Insurance £1,000,000 per claim for errors and omissions in professional advisory services, Public Liability Insurance £1,000,000 per claim for third-party injury or property damage, and Employers Liability Insurance £5,000,000 as required by UK law for employee injury or illness. Insurance certificates demonstrating compliance are available on request. The company is registered with the Information Commissioner's Office (ICO) as a data controller under registration number ZA796363 with registration maintained annually and compliance confirmed through internal audits and documented procedures.

Conflict of Interest and Independence

IVARTY operates an independent advisory model with separation between advisory and operational implementation. The firm does not provide managed security services (SOC/NOC operations), sell security products or platforms, or implement security technologies where IVARTY would benefit financially from specific technology selection recommendations. This independence ensures that security assessments, architecture recommendations, and technology selection guidance are objective and aligned to customer best interests rather than supplier commercial objectives. Where security assessments identify need for implementation support (SIEM deployment, endpoint security rollout, firewall configuration), customers are free to engage any qualified supplier including IVARTY for implementation advisory, but IVARTY does not mandate or receive referral fees from specific technology vendors. Assessment findings and risk ratings are determined objectively based on evidence against framework criteria, not influenced by potential implementation revenue. Customers can verify IVARTY's independence through transparent disclosure of any vendor relationships or technology partnerships, with no undisclosed commercial relationships that could influence advisory recommendations.

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
Established: 2017

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

Customer references available on request for verification purposes. CCS may request contact details for reference checks during evaluation.