IVARTY Consulting Ltd – Risk, Compliance & Resilience

Terms & Conditions

G-Cloud 15 Lot 3

VERSION 3.0 JANUARY 2026

Introduction & Company Details

1. Introduction

These Terms & Conditions ("T&Cs") govern the provision of the Risk, Compliance & Resilience cyber security and advisory service by IVARTY Consulting Ltd ("Supplier") to the Customer under the CCS G-Cloud 15 Framework, Lot 3 – Cloud Support. They should be read alongside the applicable Statement of Work (SoW), Pricing Document, and Service Definition, which form part of the agreement.

---

2. Company Details

Company Name IVARTY Consulting Ltd	**Registered in Scotland** SC579411
VAT Number 481446578	**Established** 2017

Registered Office: 15 Paterson Way, Cambusbarron, Stirling FK7 9RF, UK

ICO Registration: ZA796363

Scope of Services & Service Delivery

3. Scope of Services

The Supplier shall provide the Risk, Compliance & Resilience cyber security and advisory services in accordance with the agreed SoW. Services include cyber security assessment and posture improvement, compliance framework implementation (ISO 27001, Cyber Essentials Plus, UK GDPR), risk management and governance, business continuity and disaster recovery planning, security architecture and design review, incident response planning and readiness, and security awareness and capability development. Any services not explicitly included in the SoW will only be delivered subject to a mutually agreed amendment.

In summary, The Supplier does not operate, monitor, or manage cloud services or security controls.

---

4. Service Delivery

Services are delivered remotely by default, with on-site delivery (such as site visits for physical security assessments, penetration testing from customer premises, or stakeholder workshops) as agreed in the SoW.

Supplier personnel will adhere to agreed timelines, standards, and governance arrangements including security assessment methodologies aligned to NIST Cybersecurity Framework, ISO 27001, CIS Controls, and NCSC Cyber Assessment Framework.

Customer Requirements

Customers shall provide timely 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, 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 locations). Network access for vulnerability scanning or penetration testing requires firewall rule changes and change control approvals.

Charges, Payment & Customer Obligations

5. Charges, Payment & VAT

Fees are as set out in the Pricing Document and agreed SoW.

All fees are exclusive of VAT, which will be applied at the prevailing UK rate.

Payment is due within **30 calendar days** of invoice receipt unless otherwise stated in the SoW.

Expenses (travel, subsistence, accommodation) are included within day rates for remote-first delivery model. Where exceptional expenses are required beyond standard delivery assumptions (such as extended on-site penetration testing requiring overnight accommodation), these will be agreed in the SoW and charged at cost.

---

6. Customer Obligations

The Customer shall:

System & Data Access

Provide access to systems, data, documentation, and personnel as reasonably required for security assessments, including configuration exports, vulnerability scan permissions, log samples, security policies, architecture documentation, and stakeholder availability for interviews and workshops.

Network Access Facilitation

Facilitate network access for vulnerability scanning or penetration testing including firewall rule changes, scanning windows coordinated with operations teams, and change control approvals with adequate lead time for planning and coordination.

Liaison Appointment

Appoint a liaison or sponsor to facilitate engagement and coordinate stakeholder access, typically the CISO, Senior Information Risk Owner (SIRO), Information Assurance Manager, or Head of ICT.

Timely Decisions

Ensure timely decisions and approvals to enable the Supplier to meet agreed milestones, including governance board approval timescales where security policies, risk assessments, or incident response plans require formal adoption by senior leadership or audit committees.

Confidentiality, Data Protection & Intellectual Property

7. Confidentiality

Both parties shall treat all information disclosed under this engagement as confidential and shall not disclose it to third parties except as required by law or agreed in writing. This includes commercially sensitive security posture data, vulnerability assessment findings, penetration testing results, risk registers, incident logs, security architecture documentation, and technical configuration details that could be exploited if disclosed.

---

8. Data Protection & Security

Supplier complies with UK GDPR, Data Protection Act 2018, and applicable cybersecurity standards including Cyber Essentials certification (certificate CE-2024-1147-IVARTY, valid until 15 March 2026).

Personal and sensitive data processed in connection with the services (including security assessment data, vulnerability scan results, penetration testing findings, incident logs, and employee information used in awareness assessments) will be handled only for the purpose of delivering the SoW and will be processed within UK/EU with data residency guarantees.

> **Security Assessment Data Classification:** Security assessment data including vulnerability findings, penetration testing results, and configuration weaknesses is classified as sensitive and subject to enhanced protection including encryption in transit and at rest using AES-256 or equivalent, access controls limiting data to named consultants on need-to-know basis, and secure deletion using certified data destruction services upon engagement completion.

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 purposes or ongoing security advisory relationships where periodic reassessment is planned.

Customer retains responsibility for internal policies and employee data governance.

---

9. Intellectual Property

Pre-existing IP remains the property of the respective party. Security assessment frameworks, methodologies, scoring criteria, evaluation templates, and proprietary tools remain the intellectual property of IVARTY Consulting Ltd.

Deliverables created for the Customer under the SoW (including security assessment reports, compliance gap analyses, risk registers, security policies and procedures, incident response plans, business continuity plans, security architecture documentation, and remediation roadmaps) are licensed for the Customer internal use only, unless otherwise agreed in writing.

Security assessment methodologies and frameworks are IVARTY intellectual property enabling consistent delivery across customers and ensuring assessment quality, calibration, and objectivity. Customers receive assessment outputs and recommendations but not underlying assessment engines, scoring algorithms, or benchmarking databases.

Templates, toolkits, and guidance materials provided to the Customer for ongoing security self-assessment, compliance monitoring, or incident management are licensed for internal use and may not be commercialised or redistributed to third parties.

Liability, Term, Exit & Governance

10. Liability & Indemnity

Supplier liability is limited to the total fees paid under the applicable SoW, except in cases of death, personal injury, fraud, or fraudulent misrepresentation where liability is unlimited.

Neither party shall be liable for indirect or consequential loss including loss of profits, loss of business, loss of reputation, or loss of opportunity.

Insurance Coverage

The Supplier 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
- Employers Liability Insurance £5,000,000

Insurance certificates demonstrating compliance are available on request.

Customer Indemnity

The Customer indemnifies the Supplier against claims arising from misuse of deliverables or services, including claims arising from Customer implementation of security recommendations outside the scope of advisory services provided (such as firewall configuration, endpoint deployment, or SIEM implementation undertaken by Customer or third-party suppliers based on IVARTY recommendations).

Assessment Validity: Security assessments and penetration testing reflect organisational security posture at the time of assessment. The Supplier is not liable for security incidents occurring after assessment completion, changes in threat landscape, emergence of new vulnerabilities, or organisational changes affecting security posture. Customers are responsible for implementing recommended security improvements, maintaining security controls, and conducting periodic reassessments to verify continued effectiveness.

---

11. Term, Exit & Transition

Services commence on the agreed start date and continue until the end date in the SoW. Security assessments are point-in-time evaluations with validity typically 12 months, after which reassessment is recommended to verify continued compliance and identify new risks or vulnerabilities.

On termination or expiry, Supplier will:

01

Transfer Deliverables

Transfer all deliverables, reports, and documentation (security assessment reports, compliance gap analyses, risk registers, security policies, incident response plans, penetration testing results, remediation roadmaps) in machine-readable formats suitable for Customer archiving, ongoing use, and presentation to governance boards or external auditors.

02

Knowledge Transfer

Provide knowledge transfer as agreed in the SoW, including explanatory sessions on assessment findings and risk ratings, remediation plan implementation guidance, tools and templates for ongoing security self-assessment, and training for customer security teams on maintaining security posture.

03

Secure Data Deletion

Securely delete or return Customer data including vulnerability assessment results, penetration testing findings, security configuration exports, incident logs, risk assessment data, and any commercially sensitive information in accordance with UK GDPR requirements and using certified data destruction services.

04

Post-Engagement Support

Offer 30 days post-engagement support at no additional cost for clarification queries, implementation guidance, or technical questions related to deliverables.

Where ISO 27001 implementation support has been provided, provide clear guidance on certification timelines, internal audit requirements, management review cycles, and transitional arrangements if the Customer chooses not to continue the advisory relationship before certification is achieved.

---

12. Amendments & Variations

Any amendments to these T&Cs or the SoW must be agreed in writing by authorised representatives of both parties. Variations in scope, deliverables, timescales, or resource allocation are managed through formal change control process documented in the SoW.

---

13. Governing Law & Dispute Resolution

These T&Cs are governed by the laws of Scotland.

Parties shall use reasonable endeavours to resolve disputes amicably through escalation to senior management before recourse to courts or arbitration.

Disputes regarding security assessment findings or risk ratings are resolved through independent peer review by external security specialist with CISSP, CISM, or equivalent professional qualification, with peer review costs shared equally between parties.

---

14. Insurance & Professional Standards

The Supplier maintains the following insurance coverage throughout the contract term:

Insurance Type	Coverage	Purpose
Professional Indemnity Insurance	£1,000,000 per claim	Errors and omissions in professional advisory services including security assessments, compliance gap analyses, and risk management advice
Public Liability Insurance	£1,000,000 per claim	Third-party injury or property damage
Employers Liability Insurance	£5,000,000	Employee injury or illness (UK law requirement)

Aggregate cover totals **£7,000,000** exceeding G-Cloud 15 Lot 3 minimum requirements. Insurance is renewed annually with continuous cover maintained. Certificates demonstrating current coverage are available on request.

Professional Qualifications

All security assessments are conducted by qualified practitioners holding professional certifications appropriate to their role including CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional), CREST (for penetration testing), or equivalent professional qualifications demonstrating competence in cyber security assessment, risk management, or compliance frameworks.

Quality assurance of all deliverables is provided by the Chief Information Security Officer or Lead Security Architect with independent peer review for complex or high-risk assessments ensuring objectivity, calibration, and technical accuracy, as detailed in the Service Definition.

---

15. Framework Compliance & Document Hierarchy

Services are delivered in accordance with the CCS G-Cloud 15 Framework Agreement. In the event of conflict between documents, the order of precedence is:

G-Cloud 15 Framework Agreement
Governs overall relationship

Call-Off Contract
Governs specific engagement

Statement of Work
Takes precedence for engagement-specific terms, deliverables, and timescales

Pricing Document
Governs commercial and pricing matters

Service Definition
Governs scope, capabilities, and delivery approach

Terms & Conditions
Governs contractual terms not specified in higher-precedence documents

---

16. Contact Details

IVARTY Consulting Ltd
15 Paterson Way, Cambusbarron, Stirling FK7 9RF, UK
Email: steve@ivartyconsulting.com
Company Registration: SC579411
VAT Number: 481446578
ICO Registration: ZA796363

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