

Security, Compliance & Cloud Assurance Services

1. Service Overview

Security, Compliance & Cloud Assurance Services provide professional consultancy support to help organisations assess, design, and assure cloud security and compliance. The service supports buyers in identifying risks, aligning controls to requirements, and gaining assurance over cloud environments.

The service is advisory and time-bound. It does not include managed security services or ongoing operational responsibility.

2. Service Scope

The service may include the following activities:

- Cloud security strategy development
- Security risk and threat assessments
- Cloud security architecture and control design
- Compliance and regulatory assessments
- Security audit and assurance reviews
- Policy and standards alignment
- Security gap analysis
- Control effectiveness reviews
- Assurance reporting and recommendations
- Stakeholder workshops and reviews

All activities are delivered as professional services and tailored to buyer requirements agreed at call-off.

3. What the Service Includes

- Professional security and compliance consultancy
- Assessments, reviews, and assurance activities
- Written reports and recommendations
- Knowledge transfer and engagement close-out

4. What the Service Does Not Include

The service does **not** include:

- Managed security or monitoring services
- Continuous compliance tooling
- Incident response or forensic services
- Security software or licences
- Third-party services unless explicitly agreed

These services may be procured separately if required.

5. Service Delivery Model

- Delivered onsite, remotely, or using a hybrid approach
- Engagements are time-bound and scoped at call-off
- Delivered using time and materials, fixed price, or drawdown models
- Resource mix, duration, and deliverables agreed before commencement

6. Onboarding

Engagements begin with a mobilisation phase, which may include:

- Confirmation of security and compliance objectives
- Agreement of scope, governance, and stakeholders

- Identification of access and documentation requirements
- Scheduling of assessment and review activities

A delivery plan is agreed prior to work starting.

7. Exit and Offboarding

At the end of the engagement:

- All agreed outputs and reports are delivered to the buyer
- Findings and recommendations are presented
- Knowledge transfer activities are completed
- Buyer data is returned or securely deleted as agreed
- No ongoing service commitment applies beyond the engagement

8. Security and Data Handling

- Consultants follow buyer security and access policies
- Access to systems and data is limited to agreed scope
- Buyer information is handled securely and confidentially
- Data protection and confidentiality requirements are followed

9. Service Constraints and Dependencies

- Delivery depends on access to systems, documentation, and stakeholders
- Outputs are advisory and based on information available at the time
- Assurance outcomes depend on buyer implementation decisions

10. Pricing

Pricing is agreed at call-off and may be based on:

- Time and materials (daily rates)
- Fixed-price assurance or audit engagements
- Drawdown consultancy days

Pricing excludes VAT and third-party costs unless otherwise agreed.

11. Service Management and Governance

- Engagement governance is agreed at call-off
- Progress reporting is provided throughout delivery
- Issues and risks are managed through agreed escalation routes

12. Contact and Support

Support during the engagement is provided through the agreed delivery team. Any post-engagement support must be agreed separately.