

Service Definition – Security Support Software

Fimatix UK Ltd

G-Cloud 15 Lot 3 Cloud Support

Cloud Security Support Services

Supplier

Fimatix UK Ltd

Service overview

This service supports public-sector organisations to design, implement, assure, and manage security across cloud-based digital services. It provides specialist security advisory, design, risk management, and assurance capabilities aligned to public-sector governance, regulatory requirements, and cloud best practice.

The service is suitable for organisations delivering or operating cloud services that require structured security strategy, assurance, and ongoing risk management without transferring accountability away from the buyer.

Security strategy

Fimatix provides security strategy support to help organisations define clear, proportionate security objectives aligned to business goals and risk appetite. This includes:

- Development of cloud security strategies and roadmaps
- Alignment with organisational governance and policy frameworks
- Support for compliance with relevant standards and guidance (e.g. ISO/IEC 27001, NCSC guidance)
- Integration of security considerations into digital and cloud transformation programmes

Security risk management

The service supports identification, assessment, and management of security risks throughout the service lifecycle. Activities may include:

- Security risk assessments and threat modelling

- Identification and prioritisation of security risks and mitigations
- Ongoing risk tracking and reporting
- Support for security decision-making and governance forums

Security design

Fimatix supports secure-by-design approaches for cloud services and platforms. This includes:

- Security architecture and design reviews
- Identity and access management design support
- Secure DevSecOps design and integration
- Review of cloud configurations and security controls

Security design activities are proportionate to service risk and complexity.

Security incident management

The service provides advisory and support capabilities for security incident management, including:

- Support for defining incident response processes and playbooks
- Assistance during security incidents to support investigation and containment
- Post-incident reviews and lessons learned
- Recommendations to reduce the likelihood or impact of future incidents

The service does not provide a managed SOC or 24/7 monitoring unless explicitly agreed.

Security audit services

Fimatix provides independent security audit and review services to support assurance and oversight. This includes:

- Security control reviews and gap analysis
- Evidence gathering and review to support audits or assessments
- Review of security documentation, policies, and procedures

- Support for internal and external audit activities

These services support assurance but do not constitute formal certification.

Security quality assurance (QA) and testing

The service supports security assurance and testing activities, including:

- Security-focused quality assurance within delivery programmes
- Review of security requirements and acceptance criteria
- Support for vulnerability assessment and remediation planning
- Oversight of security testing activities and reporting of findings

Formal penetration testing or accreditation services are not included unless explicitly agreed.

Typical use cases

Buyers typically use this service when:

- Establishing or reviewing cloud security strategies
- Managing security risk in complex cloud programmes
- Designing secure cloud architectures and DevSecOps pipelines
- Responding to or learning from security incidents
- Preparing for audits, assessments, or assurance reviews

Service delivery approach

Delivery is collaborative and aligned to the buyer's governance structures. Security specialists work alongside delivery teams and stakeholders to provide proportionate advice, assurance, and support.

The service focuses on enabling informed decision-making, transparency of risk, and practical security improvement rather than compliance for its own sake.

Data protection and information assurance

Fimatix operates an information security and quality management framework aligned with ISO/IEC 27001 and ISO 9001 and holds Cyber Essentials certification. Services are delivered in accordance with UK GDPR and the Data Protection Act 2018.

Any access to systems or data is agreed in advance and limited to what is necessary for service delivery.

Onboarding and offboarding

At service start, scope, objectives, access requirements, and governance arrangements are agreed. A named security lead acts as the primary point of contact.

At service end, agreed outputs and documentation are transferred to the buyer, and access is removed in line with agreed offboarding processes.

Service levels

This is a professional security support service and does not include technical uptime or availability SLAs. Performance is managed through agreed objectives, milestones, and regular service reviews.

Pricing and commercial model

The service is typically delivered on a time-and-materials basis using SFIA-aligned day rates. Fixed-price delivery for defined security outcomes may be agreed where appropriate.

Invoicing is monthly in arrears.

Service constraints

- This service provides advisory, design, and assurance support and does not include managed security operations
- Final security and risk decisions remain with the buyer
- Effectiveness depends on timely access to stakeholders, systems, and information
- The service does not provide formal certification or accreditation

Customer responsibilities

Buyers are responsible for:

- Providing access to relevant systems, documentation, and stakeholders
- Making timely decisions based on security advice
- Operating and maintaining live security controls unless otherwise agreed

Experience

Fimatix has supported UK public-sector organisations with cloud security strategy, risk management, assurance, and incident support across complex digital and cloud-enabled programmes.

References and case studies are available on request.