# Service Definition Document

## Lifebit Security Services

*(Prepared for G-Cloud 15 – Cloud Support Services)*

---

## 1. What the service is

Lifebit Security Services provide specialist advisory and professional services to help customers design, assess, and operate secure cloud environments. The service covers security strategy, risk management, secure architecture design, incident management support, security audit services, and security quality assurance and testing. Services are delivered as optional professional services and scoped at call-off to support customer security, compliance, and governance requirements.

## 2. Data backup, restore, and disaster recovery

Lifebit Security Services do not manage or store customer operational data. Backup, restore, and disaster recovery remain the responsibility of the customer and their chosen cloud provider. Where required, Lifebit can assess or validate backup and recovery controls as part of security assurance or audit activities.

## 3. Onboarding and offboarding support

Onboarding includes agreement of service scope, security objectives, access requirements, and delivery timelines. Offboarding includes completion of agreed security activities, delivery of reports or recommendations, and confirmation of service closure. No data migration or technical offboarding is required as part of this service.

## 4. Service constraints

The service is delivered within customer-owned cloud environments and is subject to approved regions, security policies, and resource limits. Services are provided remotely unless otherwise agreed. Managed or ongoing security services are optional and scoped at call-off. Lifebit does not take ownership of customer cloud accounts or infrastructure unless explicitly agreed.

## 5. Service levels

Support is provided during standard UK business hours. Requests are prioritised by severity. Major incidents impacting delivery of agreed services receive an initial response within two

business hours. High- and medium-priority requests receive an initial response within four business days. Specific service levels are agreed and documented at call-off.

## 6. After-sales support

After completion of security engagements, Lifebit provides reports, findings, and recommendations. Follow-up support, remediation guidance, and re-assessment services can be provided as optional services where required.

## 7. Technical requirements

Customers must provide appropriate access to relevant cloud environments, documentation, and security controls required to deliver the agreed services. Secure connectivity and customer-managed identity and access management are required. No additional software licences are required beyond customer-selected cloud services.

## 8. Outage and maintenance management

Security services are planned to minimise disruption to customer environments. Where activities depend on customer systems or underlying cloud services, outages or maintenance by the cloud provider may affect delivery schedules and will be managed through coordination and rescheduling where necessary.

## 9. Hosting options and locations

The service is delivered within customer-owned cloud environments. Customers select hosting regions and locations to meet regulatory, data residency, and governance requirements. Lifebit does not host or retain customer data as part of this service.

## 10. Access to data upon exit

Lifebit Security Services do not restrict customer access to data. All reports, outputs, and documentation are provided to the customer. No customer data is retained following completion of the service, except where contractually required.

## 11. Security

The service is delivered in alignment with recognised security standards and cloud security best practices. Access to customer environments is controlled using customer-managed identity and access controls. Lifebit operates an ISO/IEC 27001-certified information security management system and follows defined processes for secure access, incident management, vulnerability management, and operational assurance.