Service 2: Security Risk Management

2.1 Service Overview

We provide Security Risk Management services to identify, assess, and mitigate security risks across cloud infrastructure. The service integrates security into the development lifecycle, ensuring vulnerabilities are detected early and remediated systematically.

The service combines automated scanning tools with expert review and prioritisation, aligning security remediation with delivery roadmaps to balance risk reduction with operational continuity.

2.2 Service Features

Vulnerability Scanning

- Automated scanning of AMIs and Docker images using Trivy
- AWS Inspector for image vulnerability scanning on ECR repositories
- Amazon EventBridge for capturing Inspector findings and triggers the Lambda function
- Custom Lambda function (developed and maintained by the infrastructure team) for processing Inspector findings and sends Slack notifications
- Scanning integrated into PR build pipelines for shift-left security

Security Reviews and Risk Assessment

- Periodic AWS (Cloud vendor of your choice) security and risk reviews
- Risk prioritisation based on severity, exploitability, and business impact
- Integration of security remediation into quarterly roadmap planning
- Security posture reporting for stakeholder visibility

Access and Secrets Management

- VPN access management for engineers to compute tooling and production
- Centralised secrets management via Secrets Manager
- KMS key management for encryption at rest
- IAM policy review and least-privilege enforcement

Audit and Compliance

- CloudTrail enabled for API audit logging
- Security Group and network access reviews
- VPC endpoint configuration for private AWS service access
- Evidence collection support for compliance audits

2.3 Service Benefits

Benefit	Description
Reduces security risk exposure	Automated scanning detects vulnerabilities before deployment, reducing attack surface

Reduces remediation costs	Shift-left approach catches issues early when they are cheaper and faster to fix
Improves compliance posture	Audit logging and evidence collection streamline compliance with regulatory requirements
Accelerates incident response	Automated alerting and clear ownership reduce time to detect and respond to security issues
Protects sensitive data	Centralised secrets management and encryption reduce risk of credential exposure
Provides security visibility	Regular reporting gives stakeholders clear view of security posture and risk trends
Enables secure development	Security integrated into pipelines enables teams to deliver securely without slowing down

2.4 Service Levels

Service Level	Commitment
Availability	99% uptime for managed infrastructure components
Support Hours (In-Hours)	Monday to Friday, 09:00 - 17:00 UK time (excluding public holidays)
Support Hours (Out-of-Hours)	Available, limited to runbooks supplied by individual teams
Incident Response	As agreed per engagement

2.5 Security Controls

Control Area	Implementation
Network Security	AWS Security Groups, Network Firewall, VPC Endpoints
Access Control	VPN access, IAM roles with least-privilege, MFA enforcement

Data Protection	AWS KMS encryption at rest, TLS in transit, Secrets Manager
Audit Logging	CloudTrail for API logging, log retention per compliance requirements
Vulnerability Management	Trivy and AWS Inspector scanning, prioritised remediation
Incident Management	Defined escalation paths, post-incident review process

2.6 Hosting Options and Locations

Security tooling and services operate within AWS UK regions:

- Primary region: eu-west-2 (London) can be changed per hosting specifications.
- All security logs and scan results stored within UK boundaries
- No data transferred outside UK without explicit client consent

2.7 Data Backup and Disaster Recovery

Component	Approach
Security Log Retention	90 days online, 1 year archived (configurable)
Scan Results Retention	12 months
Backup Location	Within eu-west-2 region
Recovery	Security configurations maintained as code, recoverable within RTO

2.8 Onboarding and Offboarding (people)

Onboarding

- Security baseline assessment of current environment
- Integration of scanning tools into existing CI/CD pipelines
- Configuration of alerting channels and escalation paths
- Initial risk register population and prioritisation
- Knowledge transfer on security processes and tooling

Offboarding

- Export of risk register, scan history, and security documentation
- Transfer of security tooling configuration and runbooks
- Knowledge transfer to incoming provider or internal team

- Secure deletion of access credentials and client data

2.9 Service Constraints

- Service covers AWS infrastructure security.
- Remediation of vulnerabilities is advisory; implementation responsibility agreed per engagement
- Penetration testing available as separate engagement (Specialised 3rd party engaged to provide comprehensive pen testing capabilities)
- Support provided as per section 2.4.

2.10 Outage and Maintenance Management

- Security tooling maintenance scheduled outside core hours where possible
- Planned maintenance communicated minimum 5 business days in advance
- Security incidents managed via defined incident response process
- Post-incident reports provided within 5 business days of resolution

2.11 Technical Requirements

Client technical requirements:

- AWS account with appropriate IAM permissions for security tooling
- CI/CD pipeline access for scanner integration
- Slack or Microsoft Teams for automated alerting
- Access to container registries and AMI build processes

2.12 Access to Data (Upon Exit)

Upon service termination, clients receive:

- Full export of risk register and vulnerability history
- Security scan results and trend data
- Configuration documentation for security tooling
- Audit logs for the retention period

Data provided in standard formats (JSON, CSV, PDF reports) within 10 business days of termination.