

SERVICE DEFINITION

DEVSECOPS & CLOUD SECURITY SUPPORT

DOCUMENT CONTROL

AUTHOR: PETER TEICHNER

CLASSIFICATION: CONFIDENTIAL

VERSION: 1.0

STATUS: PUBLISHED

DATE: 13/01/2026

Service Overview

DevSecOps & Cloud Security Support provides cloud support services to help public sector organisations design, deliver and assure secure cloud-based services. The service focuses on embedding security into cloud delivery through DevSecOps practices, security architecture, risk management and assurance, enabling secure-by-design and compliant cloud services.

Services are delivered at the delivery, governance and assurance layer, rather than as operational security management or hosting services.

This service is offered under G-Cloud 15 – Lot 3 (Cloud Support Services).

Scope of Service

This service supports buyers across the design, delivery and assurance lifecycle of cloud services, focusing on security practices integrated into delivery rather than operational security management.

The service includes:

- DevSecOps integration into cloud delivery pipelines
- Cloud security architecture design and assurance
- Security risk assessment and mitigation planning
- Automated security testing and validation
- Secure configuration and hardening guidance
- Security quality assurance and testing
- Security governance and assurance support

The service works alongside buyer-owned cloud platforms and third-party cloud providers, supporting outcome-focused delivery without assuming operational ownership.

Service Exclusions

The service does not include:

- Provision or ownership of cloud hosting or infrastructure
- Managed security operations or SOC services
- Real-time incident response ownership unless explicitly agreed
- Cloud licensing, subscriptions or consumption costs
- Authority to accept risk on behalf of the Buyer

Buyers retain responsibility for security governance decisions, risk acceptance and cloud platform operations.

Service Delivery Approach

Services are delivered using agile, collaborative and risk-based approaches, embedding security early and continuously throughout delivery.

Delivery activities may include:

- Assessment of existing security posture and delivery practices
- Integration of security controls into CI/CD pipelines
- Secure design reviews and threat modelling
- Hands-on delivery support and coaching
- Knowledge transfer and security documentation

Services are delivered remotely from Collabify offices by default, with on-site support available where agreed at call-off.

Service Features

- DevSecOps integration into cloud delivery pipelines
- Cloud security architecture design and assurance
- Automated security testing within CI/CD pipelines
- Security risk assessment and mitigation planning
- Secure configuration and hardening guidance
- Security quality assurance and validation
- Secure delivery process design
- Security governance and assurance

Service Benefits

- Improves security posture of cloud services
- Reduces risk of vulnerabilities and misconfiguration
- Embeds security into delivery processes
- Improves compliance with public sector requirements
- Detects security issues earlier in delivery
- Reduces remediation cost and effort
- Improves confidence in cloud service security
- Enables secure and resilient cloud

Support Levels

Support levels are flexible and agreed at call-off.

Standard support is provided during UK business hours, Monday to Friday, and includes email or ticket-based support, scheduled meetings and access to experienced cloud security and delivery specialists.

Enhanced support can be agreed where additional responsiveness or availability is required. This may include extended hours support, increased availability of specialists and priority handling of security-related requests.

Support is typically priced using transparent day rates or time-and-materials models, with fixed-price options available for defined scopes.

A named delivery lead, such as a DevSecOps lead or Cloud Security Engineer, can be provided as the primary point of coordination.

User Support

- Email or ticket-based support is available during UK business hours
- Phone support is available during UK business hours by prior agreement
- Web chat support is not provided as standard

Response times and escalation arrangements are agreed at call-off based on service context and priority.

Security and Compliance

- Staff screening is performed in line with ****BS7858:2019****
- Staff can obtain ****Security Clearance (SC)**** where required by the Buyer
- The service aligns with the NCSC Cloud Security Principles, including Personnel Security
- Secure delivery practices are embedded into DevOps workflows

Onboarding

Onboarding typically includes:

- Initial discovery and service initiation
- Confirmation of scope, objectives and success measures
- Agreement of ways of working, tooling and governance
- Access setup and knowledge transfer as required

Offboarding and Exit Management

Offboarding and exit activities are agreed at call-off and may include:

- Knowledge transfer and documentation handover
- Support for transition to internal teams or alternative suppliers
- Secure return or disposal of buyer information

Pricing

Pricing is transparent and agreed at call-off. Pricing models may include:

- Time and materials (day rates by role)
- Fixed-price delivery for defined scopes
- Optional enhanced support pricing

All pricing complies with G-Cloud framework requirements.

Service Availability

The service is available to:

- Central government departments
- Local authorities
- NHS and health bodies
- Education organisations
- Emergency services and arm's-length bodies

Discounted pricing for educational organisations can be agreed at call-off.