Service Definition Document

DevSecOps Toolchain Design and Implementation

G-Cloud 15 – Lot 3

1. Service overview

The **DevSecOps Toolchain Design and Implementation** service supports organisations to design and implement integrated DevSecOps toolchains that enable secure, automated, and efficient delivery of digital services. The service focuses on embedding security controls and quality assurance into development and deployment processes while improving delivery speed, consistency, and reliability.

The service is typically used to establish or improve DevSecOps capabilities, support cloud-native delivery, and enable repeatable, governed deployment of applications and infrastructure.

2. What the service includes

The service includes a defined set of design and implementation activities, proportionate to the agreed scope and organisational context.

Included activities

The service may include the following activities:

- Assessment of existing development, security, and deployment practices
- Design of end-to-end DevSecOps toolchains and workflows
- Selection and configuration of CI/CD tooling
- Integration of security scanning and compliance checks
- Automation of build, test, and deployment processes
- Configuration of access controls and secrets management
- Alignment of toolchains with operational and governance requirements

Key outputs and deliverables

Outputs are documented and provided to the buyer and typically include:

- Implemented DevSecOps toolchains and pipelines
- Toolchain architecture and workflow documentation

- Automated security and quality controls
- Configuration and deployment artefacts
- Operational and support handover documentation

Deliverables are designed to support secure, repeatable, and auditable delivery.

3. What the service does not include

Unless explicitly agreed as part of the call-off, the service does not include:

- Ongoing operational or managed DevSecOps services
- Application feature development beyond agreed scope
- End-user training or organisational change activities
- Procurement or resale of third-party tooling licences

These activities can be provided through related services procured separately where required.

4. How the service is delivered

The service is delivered using a structured DevSecOps implementation approach aligned to public-sector delivery and assurance expectations.

Typical delivery approach

Delivery is typically structured around the following stages:

1. **Assessment and design**
    - Review current practices and requirements
    - Define target DevSecOps toolchain and controls
2. **Toolchain implementation**
    - Configure CI/CD pipelines and automation
    - Integrate security and compliance checks
3. **Validation and testing**
    - Validate pipelines, controls, and workflows
    - Address identified issues
4. **Handover and enablement**

    - Provide documentation and knowledge transfer
    - Confirm readiness for ongoing use

Engagements typically run from **4 to 12 weeks**, depending on scope and complexity.

5. Service levels and support options

This service is delivered as a time-bound design and implementation engagement. It does not include ongoing operational or support services as standard.

Where required, post-implementation support or managed services can be agreed separately in line with standard service offerings.

6. Security, compliance and assurance

Security and compliance are central to this service and are embedded throughout the toolchain design and implementation activities, including:

- Integration of security scanning and policy enforcement
- Secure handling of credentials and secrets
- Alignment with organisational security policies and regulatory requirements

Assurance is supported through documented configurations, automated controls, and structured review of outputs.

7. Onboarding and exit

Onboarding

At the start of the engagement:

- objectives, scope, and success criteria are confirmed
- existing tooling and delivery processes are reviewed
- a delivery plan and timetable are established

Exit and handover

At completion:

- DevSecOps toolchains and pipelines are handed over
- documentation and configuration artefacts are provided

- knowledge transfer supports ongoing use and maintenance

This ensures delivery teams can operate the toolchains confidently.

8. Commercial model

The service is typically delivered on a **fixed-scope** or **time-and-materials** basis, agreed at call-off.

Scope, deliverables, and timelines are confirmed prior to delivery. Any changes to scope are managed through agreed change control.

9. Why choose this service

This service provides:

- secure and automated delivery pipelines
- embedded security and quality controls
- improved consistency and repeatability of deployments
- alignment with governance and assurance requirements

The focus is on secure, efficient, and sustainable delivery practices.

10. Next steps

To engage this service:

1. Confirm delivery objectives and tooling scope
2. Agree implementation approach and commercial model
3. Schedule assessment and design activities

The service will be tailored to reflect organisational context and delivery priorities.