the SERVER LABS

cloud architects

The Server Labs G-Cloud 15 Service Description

G-Cloud 15 Service Definition – DevSecOps Maturity Assessment for AWS

Ref: TSL/GCLOUD15/SERVICE/DEVSECOPS

Issue Number
1.0

Date
Jan 2026

DevSecOps Maturity Assessment for AWS

Overview

With over twenty years of AWS platform engineering experience, The Server Labs helps organisations understand how effectively security, automation, and governance are integrated into their software delivery pipelines.

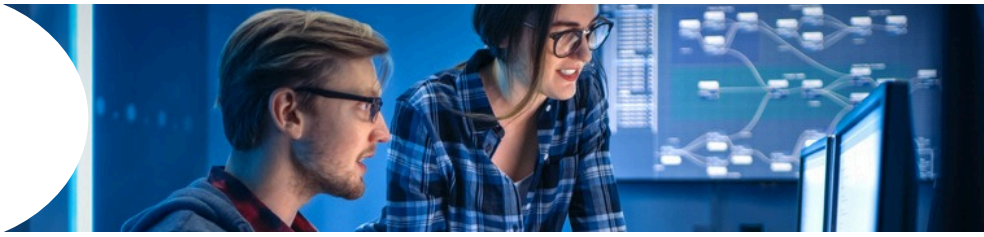
Many organisations operate CI/CD pipelines that deliver software quickly but lack consistent security controls, enforceable standards, or reliable evidence of compliance. This assessment provides a structured, engineering-led view of current DevSecOps maturity, identifying where delivery practices are creating risk, friction, or hidden operational debt.

Benefits

- Clear view of current DevSecOps maturity across the AWS estate
- Identifies where security and governance are breaking delivery flow
- Highlights risks caused by inconsistent pipelines and environments
- Focuses on engineering controls rather than process compliance
- Suitable for regulated and high-assurance environments

What this service provides

DevSecOps maturity is determined by how delivery pipelines behave in practice, not by documented processes or stated intent.
This service examines how software is currently designed, built, tested, secured, and released across the AWS environment. It focuses on CI/CD pipeline structure, automation coverage, security control integration, environment consistency, and the relationship between delivery teams and platform governance.
The assessment looks for common failure modes such as duplicated pipelines, manual approval gates, inconsistent environment configurations, security checks that block delivery rather than enable it, and assurance activities that rely on documentation instead of technical evidence.
Particular attention is given to how delivery practices scale across teams and services, and whether controls remain effective as change accelerates.
The outcome is a factual, evidence-based view of DevSecOps maturity, grounded in how delivery actually works rather than how it is described.



Who is this for

This service is suited to organisations that deliver software on AWS and need confidence that their CI/CD practices support secure, reliable, and repeatable delivery at scale.

It is particularly relevant for organisations operating in regulated, mission-critical, or high-assurance environments where security, compliance, and operational risk must be managed through engineering controls rather than manual oversight.

What's included

- Review of CI/CD pipeline structures and tooling
- Assessment of security control integration within pipelines
- Evaluation of automation coverage and manual intervention points
- Environment consistency and release risk analysis
- Governance and assurance integration review
- Identification of delivery friction and control gaps
- DevSecOps maturity baseline across teams and services
- Practical improvement backlog and prioritised recommendations

Delivery Approach

The assessment is delivered through a structured, engineering-led review of the existing delivery landscape across the AWS environment.
Work begins with analysis of current pipelines, environments, and control mechanisms to establish how software is built and released in practice. This is followed by targeted examination of where security, governance, and assurance controls are applied, how effective they are, and whether they scale consistently across teams.
Findings are consolidated into a clear maturity baseline, highlighting strengths, weaknesses, and systemic risks. Recommendations focus on practical improvements that can be implemented through platform and pipeline changes rather than additional process or manual oversight.

Key Deliverables

- DevSecOps Maturity Assessment Report covering delivery, security, and governance integration
- CI/CD pipeline maturity and risk analysis summary
- Environment consistency and release control findings
- Security and assurance integration gap assessment
- Prioritised DevSecOps improvement backlog
- Executive summary suitable for technical and leadership audiences

AWS Services & Framework Alignment

This service is aligned with the AWS Well-Architected Framework, with particular emphasis on the Security, Operational Excellence, and Reliability pillars as they relate to software delivery and automation.

The assessment typically references the following AWS services and frameworks:

- AWS Well-Architected Framework and Tool
- AWS CodePipeline, CodeBuild, and CodeDeploy
- Amazon EKS and Amazon ECS
- AWS Identity and Access Management (IAM)
- Amazon VPC and network security services
- AWS CloudWatch and logging services
- AWS Config and Security Hub
-

The specific services reviewed will vary depending on the client's delivery tooling, platform architecture, and regulatory context.

Pricing & Commercial Model

- **Engagement Model**: Professional Services
- **Pricing**: Please contact TSL for details of pricing models available
- **Procurement**: Available via G-Cloud 15 and AWS Marketplace

DevSecOps Pipeline Blueprint & Guardrail Library for AWS

Overview

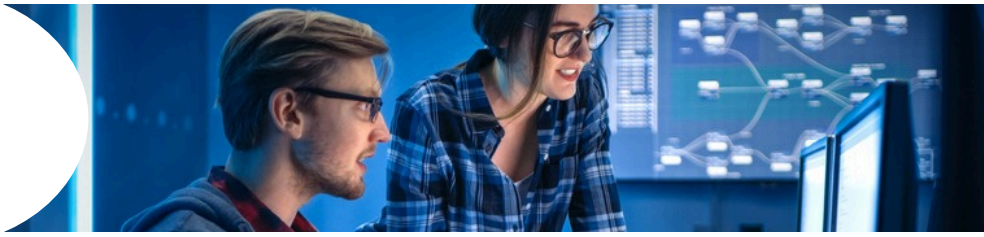
With over twenty years of AWS platform engineering experience, The Server Labs defines standardised CI/CD pipeline architectures and guardrail patterns that make security, governance, and quality enforceable through delivery.
Many organisations operate multiple pipelines that have evolved independently, resulting in inconsistent controls, fragile security integration, and delivery practices that are difficult to govern at scale. This service establishes a clear, repeatable DevSecOps blueprint for AWS, providing standard pipeline patterns and policy-as-code guardrails that enable secure, reliable delivery without introducing manual gates or process overhead.

Benefits

- Establishes a consistent DevSecOps delivery architecture
- Standardises CI/CD pipeline structure across teams
- Embeds security and governance through policy-as-code
- Reduces delivery risk caused by bespoke pipelines
- Suitable for regulated and high-assurance environments

What this service provides

Effective DevSecOps depends on having a small number of well-defined delivery patterns that teams can adopt consistently.
This service focuses on defining the target DevSecOps architecture for AWS, including how pipelines are structured, where controls are applied, and how environments are separated and promoted. It addresses the practical realities of multi-team delivery by establishing patterns that are secure by default, easy to adopt, and enforceable through automation.
The guardrail library defines technical controls that are applied through pipelines and platform services rather than manual approval processes. These controls are expressed as policy-as-code and reusable templates, allowing security, compliance, and quality requirements to be enforced consistently across services and teams.
The outcome is a set of architectural patterns that reduce variation, simplify assurance, and provide a clear foundation for secure pipeline implementation.



Who is this for

This service is suited to organisations that have completed a DevSecOps maturity assessment and require a clear, standardised delivery architecture before implementing or refactoring CI/CD pipelines.
It is particularly relevant for organisations operating in regulated or high-assurance environments where delivery controls must be consistent, enforceable, and demonstrable across teams.

What's included

- Target DevSecOps reference architecture for AWS
- Standard CI/CD pipeline patterns and templates
- Environment separation and promotion models
- Control insertion points across the delivery lifecycle
- Policy-as-code guardrail definitions
- Security, quality, and compliance control mapping
- Architecture governance artefacts for delivery adoption

Delivery Approach

The engagement is delivered through structured architectural design focused on translating delivery, security, and governance requirements into practical pipeline and guardrail patterns.

Work begins by defining a small number of standard pipeline models aligned to the organisation's delivery tooling and AWS environment. Guardrails are then designed to integrate security, compliance, and quality controls directly into those pipelines. Patterns are reviewed and refined to ensure they are implementable, scalable, and compatible with existing operating models.
The resulting blueprints are documented clearly so that implementation teams can adopt them consistently across services and environments.

Key Deliverables

- DevSecOps Pipeline Blueprint defining standard delivery patterns
- Guardrail Library with reusable policy-as-code templates
- Environment separation and promotion architecture
- Control mapping across build, test, and release stages
- Architecture governance summary for adoption and rollout

AWS Services & Framework Alignment

This service is aligned with the AWS Well-Architected Framework, with particular emphasis on the Security, Operational Excellence, and Reliability pillars as they apply to CI/CD and automated delivery.

Architectural designs typically reference the following AWS services and frameworks:

- AWS Well-Architected Framework and Tool
- AWS CodePipeline, CodeBuild, and CodeDeploy
- Amazon EKS and Amazon ECS
- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudFormation or Terraform
- Amazon VPC and network security services
- AWS CloudWatch

The specific services and patterns used will vary depending on the client's delivery tooling, platform architecture, and regulatory context.

Pricing & Commercial Model

-**Engagement Model**: Professional Services
-**Pricing**: Fixed-price or Time & Materials (depending on complexity)
-**Procurement**: Available via G-Cloud 15 and AWS Marketplace

DevSecOps Automation & Evidence Integration for AWS

Overview

With over twenty years of AWS platform engineering experience, The Server Labs integrates security, compliance, and quality controls directly into CI/CD pipelines so that assurance evidence is generated automatically through delivery activity.

Many organisations rely on manual checks, retrospective reviews, or documentation-heavy processes to demonstrate compliance and control. This service replaces those approaches with engineered automation, embedding evidence generation into pipelines so that assurance becomes a by-product of normal software delivery rather than a separate activity.

Benefits

- Embeds security and compliance controls directly into delivery pipelines
- Automates generation of technical assurance evidence
- Reduces reliance on manual checks and documentation
- Improves delivery flow while strengthening control effectiveness
- Suitable for regulated and high-assurance environments

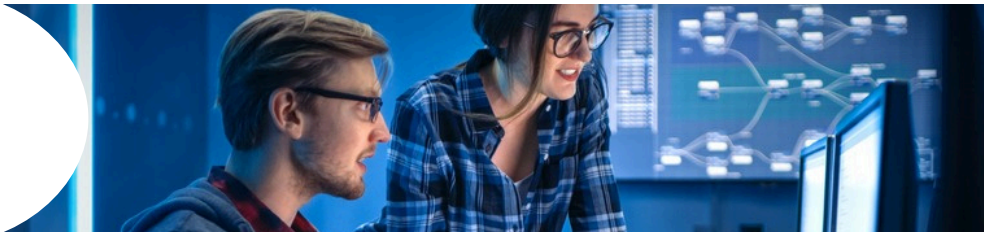
What this service provides

Assurance is most effective when it is produced by systems rather than people.

This service focuses on implementing automated controls and evidence generation within CI/CD pipelines, aligned to the agreed DevSecOps architecture and guardrail patterns. Security, quality, and compliance checks are integrated at appropriate points in the delivery lifecycle so that evidence is created continuously as code moves through build, test, and release stages.

The work emphasises technical evidence derived from pipeline execution, platform configuration, and control outcomes, rather than written attestations or manual sign-off. This approach improves confidence in the integrity of delivery while reducing friction for engineering teams.

The result is a delivery environment where assurance is continuous, repeatable, and demonstrable without slowing development.



Who is this for

This service is suited to organisations that have established standard pipeline patterns and now need to integrate enforceable controls and automated evidence into their delivery processes.

It is particularly relevant for regulated, mission-critical, or high-assurance environments where reliable, repeatable evidence of control effectiveness is required as part of normal operations.

What's included

- Integration of security and quality controls into CI/CD pipelines
- Automated policy enforcement and control validation
- Evidence generation aligned to delivery activity
- Configuration of reporting and traceability mechanisms
- Reduction of manual approval and assurance steps
- Alignment with existing governance and risk frameworks

Delivery Approach

The engagement is delivered as a focused engineering sprint designed to integrate automation and evidence generation into existing delivery pipelines.

Work begins with identification of the controls and assurance requirements that must be enforced through delivery. These controls are then implemented directly within CI/CD pipelines using automation and policy-as-code techniques. Evidence generation is validated to ensure it is reliable, traceable, and suitable for assurance and regulatory purposes.

The resulting automation is designed to be reusable and maintainable so that evidence continues to be produced consistently as delivery practices evolve.

Key Deliverables

- CI/CD pipelines with integrated security and compliance controls
- Automated evidence generation mechanisms
- Control and policy enforcement configurations
- Traceability and reporting outputs suitable for assurance
- Documentation of implemented controls and evidence sources

AWS Services & Framework Alignment

This service is aligned with the AWS Well-Architected Framework, with particular emphasis on the Security, Operational Excellence, and Reliability pillars as they relate to automated delivery and assurance.

Implementation typically references the following AWS services and frameworks:

- AWS Well-Architected Framework and Tool
- AWS CodePipeline, CodeBuild, and CodeDeploy
- AWS Identity and Access Management (IAM)
- AWS Config and Security Hub
- Amazon EKS and Amazon ECS
- AWS CloudWatch and logging services
- Infrastructure-as-code tooling

The specific services and controls used will vary depending on the client's delivery tooling, platform architecture, and regulatory context.

Pricing & Commercial Model

-**Engagement Model**: Professional Services
-**Pricing**: Fixed-price or Time & Materials (depending on complexity)
-**Procurement**: Available via G-Cloud 15 and AWS Marketplace

Managed DevSecOps Continuity Wrap for AWS

Overview

With over twenty years of AWS platform engineering experience, The Server Labs provides ongoing architectural oversight to sustain DevSecOps delivery standards as platforms, teams, and workloads evolve.
Even well-designed DevSecOps pipelines and guardrails can degrade over time as new services are introduced, teams change, and requirements shift. This service ensures that delivery patterns, controls, and automation remain effective, enforceable, and aligned with the organisation's evolving AWS platform.

Benefits

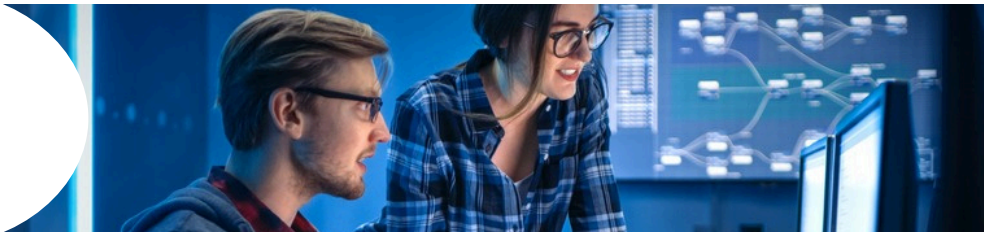
- Prevents drift in CI/CD pipelines and delivery controls
- Sustains security and governance effectiveness over time
- Maintains consistency as teams and services scale
- Provides architectural assurance without delivery friction
- Supports long-term platform and delivery stability

What this service provides

DevSecOps is not a one-time implementation; it is an operating capability that must be maintained deliberately.

This service provides structured, ongoing oversight of DevSecOps pipelines, guardrails, and automation mechanisms to ensure they continue to operate as intended. It focuses on identifying drift, erosion of controls, or emerging risks caused by platform change, new delivery patterns, or evolving security and compliance requirements.

The service reviews how pipelines are being used in practice, whether guardrails remain effective, and whether evidence generation continues to provide reliable assurance. Where gaps or weaknesses are identified, targeted recommendations are provided to restore consistency and control without introducing additional process or overhead. The emphasis is on sustaining delivery excellence through engineering discipline rather than manual oversight.



Who is this for

This service is suited to organisations that have implemented DevSecOps pipeline patterns and automation and need confidence that those approaches remain effective as delivery scales and changes over time.

It is particularly relevant for regulated, mission-critical, or high-assurance environments where delivery controls must remain enforceable and demonstrable throughout the platform lifecycle.

What's Included

- Ongoing architectural review of CI/CD pipelines
- Guardrail and policy effectiveness checks
- Drift detection across delivery tooling and environments
- Review of automated evidence and assurance outputs
- Recommendations for control and pipeline refinement
- Support for evolving delivery and platform requirements
- Executive-level assurance summaries

Delivery Approach

The engagement is delivered as a lightweight but structured continuity service focused on how DevSecOps operates in production.

Regular reviews examine pipeline usage, control enforcement, and evidence generation across the AWS environment. These reviews are designed to identify emerging risks early, before they impact delivery speed, security posture, or compliance confidence.

Findings are translated into clear, actionable recommendations that can be implemented by internal teams or through follow-on engineering support. The approach maintains momentum and discipline without introducing additional delivery gates or operational burden.

Key Deliverables

- DevSecOps continuity and drift assessment summaries
- Guardrail and control effectiveness reports
- Pipeline usage and consistency findings
- Targeted improvement recommendations
- Executive-level assurance updates

AWS Services & Framework Alignment

This service is aligned with the AWS Well-Architected Framework, with particular emphasis on the Security, Operational Excellence, and Reliability pillars as they apply to sustained delivery practices.

Continuity activities typically reference the organisation's existing AWS delivery and platform services, commonly including:

- AWS Well-Architected Framework and Tool
- AWS CodePipeline, CodeBuild, and CodeDeploy
- Amazon EKS and Amazon ECS
- AWS Identity and Access Management (IAM)
- AWS Config and Security Hub
- AWS CloudWatch and logging services

The specific services reviewed will vary depending on the client's delivery tooling, platform architecture, and regulatory context.

Pricing & Commercial Model

-**Engagement Model**: Professional Services
-**Pricing**: Fixed-price or Time & Materials (depending on complexity)
-**Procurement**: Available via G-Cloud 15 and AWS Marketplace

the SERVER LABS
cloud architects

TSL Company Profile

Founded in 2004, TSL are cloud architects and integrators.

We offer a full range of lifecycle cloud solutions and services, from consultancy, software/application development, to cloud architecture design, and integration, to fully managed services.

Our specialisations are High Performance Computing and AI/ML deployed in highly secure cloud environments, with best practice built in from day one.

Our clients include private and public organisations, with an emphasis on those processing large amounts of data in mission critical environments, particularly in the Lifesciences, Utilities, Banking, Space, Metrology and Telecoms sectors.

aws PARTNER Advanced Tier Services

aws PARTNER Migration and Modernization Services

aws PARTNER Well-Architected Partner Program

CfA Centre for Assessment ISO 27001 Information Security

UKAS MANAGEMENT SYSTEMS 0120

CYBER ESSENTIALS PLUS

The Server Labs 3 Layer Service Map

AI Readiness

- **Ultra Compute** — Scalable, Burstable, Parallel Compute Orchestration
- **Data Fabric** — Massive Scale, Optimised, Multimodal Data Platforms

Cloud Maturity Accelerators

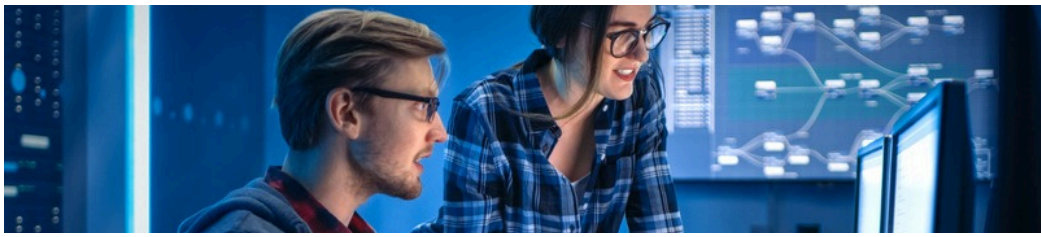
- Cloud Migration Factory & Migrations
- Cloud Adoption Accelerator & Landing Zones
- Cloud Modernisation & Optimisation Toolkits
- Cloud Centre Of Excellence Rollout Accelerator

Trusted Foundations

- Zero-Trust Security Blueprint & Security Hardening Toolkit
- FinOps and Sustainability Toolkit
- Backup, Resilience & SRE Best Practice Blueprints
- Sovereignty & Regulatory Compliance Toolkits
- Modern DevSecOps Automation Practices
- Well Architected

the SERVER LABS

cloud architects



The Company's mission is:

- To provide expert services in the field of cloud architectures, High Performance Computing, and advanced cloud software engineering
- To radically improve cloud software development processes
- To help organisations achieve better business results through the correct use of cloud technologies
- To create high quality innovative cloud software solutions, providing added value to our customers

The specific value, experience and expertise that The Server Labs can provide are:

1. **Technical excellence** and capability to act as lead on architectural decisions and as technology expert in software and system subjects.
2. **Proven experience** in implementing HPC, FinOps, Cloud Security and Big Data Projects.
    - FinOps sustainable change management to enable innovation
    - Industry leading experts in high performance computing
    - Cloud security and sensitive, big data management and processing
3. **Cloud migration**: Proven track record in migrating large, complex and sensitive dataset from on-premise to cloud environments and from legacy to target cloud.
4. **Architecture experience** at software and system level.

AWS MAP and WAF certified

TSL have achieved AWS MAP competence, which is a rigorous and demanding standard to achieve and few boutique consultancies like TSL have achieved this.

Our architects and engineers are experts with an average of 10 years' experience in the planning, design and development of complex software systems. Our multinational team has been a pioneer in cloud native service, serverless computing, automation, infrastructure as code, and distributed architectures, and has the required hands-on experience in many state of the art technologies.

The Server Labs is a leader in cloud computing solutions and services, helping organisations to move to the cloud at all levels.

Ready to lead the future?

Explore what's possible with TSL—
where innovation meets execution.
Contact us today to start your journey.

Visit our website | Email us

the SERVER LABS
cloud architects

United Kingdom

The Server Labs Ltd.
10 Bloomsbury Way London
WC1A 2SL United Kingdom

+44 (0)203 948 1082

Germany

The Server Labs Berliner
Allee 47, 64295 Darmstadt,
Germany

+49 6151 277 6037

Spain

The Server Labs S.L.
C/Maria de Molina, 39
28006 Madrid, España

+34 91 745 68 77