SERVICE DEFINITION

CROWN COMMERICAL SERVICE
G-CLOUD 15
LOT 3 - CLOUD SUPPORT

CLOUD SECURITY HARDENING AND SECOPS ENABLEMENT

TRANSFORMCX LIMITED

JANUARY 30, 2026
CONTACT: GOV@TRANSFORMCX.COM
WWW.TRANSFORMCX.COM

Contents

01

SERVICE OVERVIEW

The **Cloud Security Hardening and SecOps Enablement** service supports organisations to strengthen the security posture of their cloud environments and establish effective security operations practices. The service focuses on implementing security controls, improving visibility, and enabling ongoing security operations aligned to organisational policies and risk appetite.

The service is typically used to improve baseline cloud security, address identified risks, and support secure operation of cloud services as part of cloud adoption, migration, or ongoing service delivery.

02

WHAT THE SERVICE INCLUDES

The service includes a defined set of security hardening and enablement activities, proportionate to the agreed scope and organisational context.

Included activities

The service may include the following activities:

- Assessment of existing cloud security configurations and controls
- Implementation of security hardening measures across cloud services
- Configuration of identity, access, and privilege controls
- Network security configuration and segmentation
- Enablement of security monitoring and alerting
- Integration with existing security operations processes
- Alignment of security controls with organisational policies and standards

Key outputs and deliverables

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

- Hardened cloud environments and configurations

- Security configuration and control documentation
- Implemented monitoring and alerting capabilities
- Identified risks and remediation actions
- Operational security handover documentation

Deliverables are designed to support improved security resilience and operational readiness.

03

WHAT THE SERVICE DOES NOT INCLUDE

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

- Continuous security operations or managed security services
- Security incident response services beyond initial enablement
- End-user security awareness training
- Procurement or resale of security tooling licences

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

04

HOW THE SERVICE IS DELIVERED

The service is delivered using a structured security hardening and enablement approach aligned to public-sector security and assurance expectations.

Typical delivery approach

Delivery is typically structured around the following stages:

1. **Assessment and planning**
    - Review current security posture and requirements
    - Define hardening and enablement scope
2. **Security hardening**
    - Implement security controls and configurations
    - Address identified security gaps
3. **SecOps enablement**
    - Configure monitoring, alerting, and security workflows
    - Integrate with operational processes
4. **Validation and handover**
    - Validate security controls and configurations
    - Complete documentation and knowledge transfer

Engagements typically run from **4 to 10 weeks**, depending on scope and complexity.

05

SERVICE LEVELS AND SUPPORT OPTIONS

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

Where required, ongoing security operations or managed services can be agreed separately in line with standard service offerings.

06

SECURITY, COMPLIANCE AND ASSURANCE

Security and compliance are the primary focus of this service. Activities are aligned to organisational security policies, risk management approaches, and applicable regulatory requirements.

Assurance is supported through documented configurations, validation activities, and structured review of security outcomes.

07

ONBOARDING AND EXIT

Onboarding
At the start of the engagement:

- objectives, scope, and success criteria are confirmed
- cloud environments and security requirements are agreed
- a delivery plan and timetable are established

Exit and handover
At completion:

- hardened environments and security controls are handed over
- documentation and configuration artefacts are provided
- knowledge transfer supports ongoing security operations

This ensures security improvements are sustained following delivery.

08

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.

09

WHY CHOOSE THIS SERVICE

This service provides:

- improved security posture for cloud environments
- reduced exposure to common cloud security risks
- improved visibility and control for security operations
- alignment with organisational security and governance requirements

The focus is on practical, sustainable security improvement.

10

NEXT STEPS

To engage this service:

1. Confirm security objectives and environments in scope
2. Agree delivery approach and commercial model
3. Schedule assessment and planning activities

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