SERVICE DEFINITION

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

# SECURE CLOUD IDENTITY AND ACCESS OPERATIONS

TRANSFORMCX LIMITED

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

## Contents

# 01

# SERVICE OVERVIEW

The **Secure Cloud Identity and Access Operations** service supports organisations to operate, manage, and maintain identity and access controls for cloud environments on an ongoing basis. The service focuses on ensuring that access to cloud platforms, applications, and data remains secure, controlled, and aligned with organisational policies and governance requirements.

The service is typically used to support live cloud services where effective identity and access operations are critical to security, compliance, and continuity of service.

# 02

# WHAT THE SERVICE INCLUDES

The service includes a defined set of identity and access operational activities, proportionate to the agreed scope and service criticality.

**Included activities**

The service may include the following activities:

- Ongoing management of cloud identity and access configurations
- Administration of user, role, and service account access
- Management of privileged access and elevated permissions
- Support for access change requests and approvals
- Monitoring and review of access activity and entitlements
- Support for joiner, mover, and leaver processes
- Alignment of access operations with organisational policies and controls

**Key outputs and deliverables**

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

- Maintained and controlled identity and access configurations
- Access request and change records
- Privileged access logs and audit evidence
- Periodic access review and assurance reports
- Operational runbooks and procedures

Deliverables are designed to support secure, auditable access management.

# 03

# WHAT THE SERVICE DOES NOT INCLUDE

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

- Design or implementation of new identity architectures
- Procurement or resale of identity management software
- End-user training or organisational change activities
- Broader security operations beyond identity scope

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

# 04

# HOW THE SERVICE IS DELIVERED

The service is delivered using structured identity and access operational processes aligned to public-sector security and assurance expectations.

**Typical delivery approach**

Delivery is typically structured around the following activities:

1. **Service onboarding**
    - Confirm identity systems and access scope
    - Establish operational processes and controls

2. **Operational delivery**
    - Manage access requests and changes
    - Maintain identity configurations and controls

3. **Monitoring and assurance**
    - Review access activity and permissions
    - Support audits and assurance activities

4. **Service review and improvement**
    - Conduct service reviews and reporting
    - Identify and implement improvements

Support arrangements are tailored to service criticality and operational needs.

# 05

# SERVICE LEVELS AND SUPPORT OPTIONS

This service is delivered as an operational support service. Service hours, response times, escalation paths, and reporting arrangements are agreed at call-off.

Support can be provided during business hours or on a 24×7×365 basis, depending on service requirements.

# 06

# SECURITY, COMPLIANCE AND ASSURANCE

Security and compliance are central to this service and include:

- enforcement of least-privilege and access control policies
- monitoring of access activity and anomalies
- alignment with organisational security policies and regulatory requirements

Assurance is supported through access logs, review reports, and structured operational controls.

# 07

# ONBOARDING AND EXIT

**Onboarding**

At the start of the service:

- identity systems and responsibilities are confirmed
- access controls and processes are agreed
- service levels and reporting are established

**Exit and handover**

At service exit:

- identity and access responsibilities are transitioned
- documentation and operational knowledge are handed over
- continuity of access management is maintained

This supports secure and orderly transition.

# 08

# COMMERCIAL MODEL

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

Scope, service levels, and pricing are confirmed prior to service commencement. Any changes are managed through agreed change control.

# 09

# WHY CHOOSE THIS SERVICE

This service provides:

- secure and controlled access to cloud services
- reduced risk of unauthorised access
- improved auditability and compliance
- reliable operational identity management

The focus is on maintaining secure access throughout live service operation.

# 10

# NEXT STEPS

To engage this service:

1. Confirm identity systems and access scope

2. Agree operational model and service levels
3. Schedule service onboarding

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