

SERVICE
DEFINITION

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

IDENTITY AND ACCESS MANAGEMENT FOR CLOUD PLATFORMS

TRANSFORMCX
LIMITED

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

Contents

SERVICE OVERVIEW	3
WHAT THE SERVICE INCLUDES	3
WHAT THE SERVICE DOES NOT INCLUDE	4
HOW THE SERVICE IS DELIVERED	4
SERVICE LEVELS AND SUPPORT OPTIONS	5
SECURITY, COMPLIANCE AND ASSURANCE	5
ONBOARDING AND EXIT	6
COMMERCIAL MODEL	7
WHY CHOOSE THIS SERVICE	7
NEXT STEPS	8

01

SERVICE OVERVIEW

The **Identity and Access Management for Cloud Platforms** service supports organisations to design, implement, and improve identity and access controls for cloud environments. The service focuses on ensuring that users, systems, and services have appropriate access to cloud resources, aligned to security policies, least-privilege principles, and governance requirements.

The service is typically used to establish or enhance identity and access management capabilities as part of cloud adoption, migration, or ongoing cloud operations.

02

WHAT THE SERVICE INCLUDES

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

Included activities

The service may include the following activities:

- Assessment of existing identity and access management arrangements
- Design of cloud identity and access management architectures
- Configuration of identity providers and directory services
- Implementation of role-based and attribute-based access controls
- Configuration of privileged access management controls
- Integration of identity services with cloud platforms and applications
- Alignment of access controls with organisational policies and governance

Key outputs and deliverables

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

- Implemented identity and access management configurations

- Identity and access architecture documentation
- Defined roles, permissions, and access models
- Privileged access management configurations
- Validation and configuration evidence

Deliverables are designed to support secure and controlled access to cloud resources.

03

WHAT THE SERVICE DOES NOT INCLUDE

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

- Ongoing identity operations or access administration
- Continuous monitoring of identity-related security events
- End-user training or organisational change activities
- Procurement or resale of identity management software 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 identity and access management implementation 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 identity arrangements and requirements
 - Define target identity and access management approach
2. **Design**
 - Design identity architectures and access models

- Review designs with relevant stakeholders
- 3. **Implementation**
 - Configure identity services and access controls
 - Integrate identity services with cloud platforms and applications
- 4. **Validation and handover**
 - Validate access 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 design and implementation engagement. It does not include ongoing operational or support services as standard.

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

06

SECURITY, COMPLIANCE AND ASSURANCE

Security and compliance are central to this service. Activities support:

- enforcement of least-privilege access principles
- reduction of unauthorised access risks
- alignment with organisational security policies and regulatory requirements

Assurance is supported through documented access models, configuration evidence, and structured review of outputs.

07

ONBOARDING AND EXIT

Onboarding

At the start of the engagement:

- objectives, scope, and success criteria are confirmed
- identity platforms and applications in scope are agreed
- a delivery plan and timetable are established

Exit and handover

At completion:

- identity and access configurations are handed over
- documentation and configuration artefacts are provided
- knowledge transfer supports ongoing operation

This ensures access controls can be maintained effectively.

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:

- controlled and auditable access to cloud platforms
- reduced risk of unauthorised access
- improved alignment with security and governance requirements
- a consistent approach to managing cloud identities

The focus is on secure, well-governed access management.

10

NEXT STEPS

To engage this service:

1. Confirm identity objectives and systems in scope
2. Agree delivery approach and commercial model
3. Schedule assessment and design activities

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