SERVICE DEFINITION

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

BUSINESS CONTINUITY, BACKUP AND DISASTER RECOVERY FOR CLOUD

TRANSFORMCX LIMITED

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

Contents

01

SERVICE OVERVIEW

The **Business Continuity, Backup and Disaster Recovery for Cloud** service supports organisations to design, implement, and validate arrangements that protect cloud-based services against disruption, data loss, and failure. The service focuses on ensuring that critical systems can be recovered within agreed timeframes and that continuity arrangements are aligned to organisational risk appetite and operational priorities.

The service is typically used to establish or improve cloud resilience as part of cloud adoption, migration, or ongoing service assurance.

02

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 business continuity and disaster recovery arrangements
- Definition of recovery objectives, including RTO and RPO
- Design of backup, recovery, and resilience architectures
- Configuration of backup and replication services
- Design and implementation of disaster recovery approaches
- Documentation of continuity and recovery procedures
- Support for validation and testing of recovery arrangements

Key outputs and deliverables

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

- Implemented backup and recovery configurations

- Disaster recovery designs and architectures
- Documented recovery procedures and runbooks
- Evidence of backup and recovery testing
- Recommendations for ongoing resilience improvement

Deliverables are designed to support reliable recovery and continuity of service.

03

WHAT THE SERVICE DOES NOT INCLUDE

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

- Continuous backup monitoring or managed recovery services
- Execution of live disaster recovery during an actual incident
- End-user business continuity training
- Organisational crisis management activities

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 business continuity and disaster recovery implementation approach aligned to public-sector delivery and assurance expectations.

Typical delivery approach

Delivery is typically structured around the following stages:

1. **Assessment and planning**
    - Review continuity requirements and current arrangements
    - Define recovery objectives and scope
2. **Design**
    - Design backup and disaster recovery architectures
    - Agree recovery strategies and priorities
3. **Implementation**
    - Configure backup and replication services
    - Implement recovery mechanisms
4. **Testing and validation**
    - Conduct recovery testing exercises
    - Validate recovery objectives
5. **Handover**
    - Complete documentation and knowledge transfer
    - Confirm readiness for operational use

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 backup management or disaster recovery support can be agreed separately in line with standard service offerings.

06

SECURITY, COMPLIANCE AND ASSURANCE

Security and compliance considerations are addressed throughout the design and implementation of continuity and recovery arrangements, including:

- protection of backup data and recovery environments
- alignment with organisational security policies and regulatory requirements
- validation of recovery controls and processes

Assurance is supported through documented designs, testing evidence, and structured review of outcomes.

07

ONBOARDING AND EXIT

Onboarding

At the start of the engagement:

- continuity objectives and systems in scope are confirmed
- recovery requirements and dependencies are agreed
- a delivery plan and timetable are established

Exit and handover

At completion:

- continuity and recovery arrangements are handed over
- documentation and runbooks are provided
- knowledge transfer supports ongoing resilience management

This ensures recovery capabilities can be maintained and exercised.

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 resilience of cloud services
- reduced risk of data loss and prolonged outages
- clear, tested recovery arrangements
- alignment with organisational continuity and assurance requirements

The focus is on practical, reliable service resilience.

10

NEXT STEPS

To engage this service:

1. Confirm continuity 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 resilience priorities.