DRIE SECURE SYSTEMS
G-CLOUD 15 - SERVICE DEFINITION DOCUMENT

Cloud disaster recovery & resilience engineering

Service overview

The Cloud Disaster Recovery & Resilience Engineering Service helps public sector organisations design and implement proportionate, well-governed disaster recovery and resilience capabilities for cloud-hosted services. The service focuses on protecting critical services, data and operations, while providing clear assurance on recoverability, availability and operational risk.

The service is suitable for organisations operating business-critical digital services that require reliable continuity arrangements aligned to organisational risk appetite, regulatory obligations and public accountability.

Scope of the service

Depending on phase, the service may include:

- Assessment of service criticality and recovery requirements
- Definition of recovery time and recovery point objectives
- Design of disaster recovery and resilience architectures
- Implementation of backup, replication and failover mechanisms
- Automation of recovery processes where appropriate
- Testing and validation of recovery scenarios
- Documentation of recovery procedures and operational guidance

All activities are scoped and agreed in advance.

Delivery approach

Delivery follows established public sector digital and service management practices, aligned to the GDS Service Manual and agile delivery principles. Work is structured to reduce risk, provide transparency, and support informed decision-making by senior responsible owners.

Discovery

Discovery establishes current resilience posture and recovery requirements. This phase focuses on understanding service criticality, dependencies, existing architecture, recovery objectives and organisational constraints. It also considers third-party dependencies and operational responsibilities. Outputs support clear decisions on appropriate recovery approaches and investment.

Alpha

Alpha tests proposed recovery and resilience approaches in a controlled way. This may include prototyping backup and replication mechanisms, testing failover patterns, and validating recovery assumptions. Alpha is used to reduce uncertainty and confirm feasibility before full implementation.

Beta

Beta delivers a production-ready disaster recovery and resilience solution. This includes implementation of agreed recovery architectures, automation where appropriate, documentation of recovery procedures, and validation through testing. Solutions are prepared for operational use and ongoing assurance.

Each phase includes clear outputs and recommendations to support senior oversight.

Security, governance & assurance

Security and governance are embedded throughout delivery. This includes secure access controls, encryption, segregation of environments, audit logging and alignment with organisational security policies.

The service supports assurance through documented recovery objectives, tested procedures and clear operational ownership. It does not provide formal certification but supports audit and assurance activities required within the public sector.

Customer responsibilities

The customer is responsible for defining service priorities, confirming recovery objectives, providing access to systems and stakeholders, and retaining ownership of business continuity decisions. Ongoing operation and testing of recovery arrangements remain the customer's responsibility unless additional managed services are agreed.

Service outputs

Outputs are agreed by phase and may include recovery designs, implemented recovery solutions, test results, documentation and operational runbooks. Knowledge transfer supports continuity and ongoing assurance.

Exit and handover

At the end of the engagement, drie provides documentation and knowledge transfer to support continuity and sustainability. Any ongoing monitoring, retraining or support is subject to a separate agreement.

drie