

Centerprise Sovereign Disaster Recovery as a Service (DRaaS)

G Cloud 15, Jan 2026

Service Overview

Centerprise Sovereign Disaster Recovery as a Service (DRaaS) is a managed recovery service that enables rapid restoration of business-critical workloads after a major incident, system failure, or cyber event. The service provides assured recovery through Centerprise-operated UK sovereign infrastructure, enabling customers to recover services in a controlled, secure, and predictable manner.

DRaaS complements Backup as a Service by providing orchestrated recovery of protected workloads into a secure recovery environment. The service reduces downtime, supports business continuity objectives, and removes the complexity of maintaining in-house disaster recovery infrastructure.

The service is delivered as a fully managed service, with Centerprise responsible for recovery platform operation, recovery orchestration, and support throughout invocation and testing.

Service Scope and Capabilities

Centerprise DRaaS provides managed recovery for agreed workloads based on predefined recovery configurations and documented recovery procedures.

Key capabilities include:

- Secure recovery environments hosted on UK sovereign infrastructure
- Orchestrated recovery of workloads following a declared incident
- Point-in-time recovery using protected backup data
- Recovery testing and rehearsal support
- Secure network connectivity to recovered workloads
- Controlled access to recovered systems during invocation
- Post-incident transition back to primary environments

Recovery scenarios, dependencies, and priorities are defined during onboarding and documented in customer-specific recovery documentation.

Sovereign Infrastructure and Data Residency

Recovery environments are hosted within Centerprise-operated UK sovereign infrastructure. Customer data remains under UK jurisdiction and is not hosted in, or recovered to, public hyperscale cloud platforms unless explicitly agreed.

This approach supports public sector assurance, data sovereignty, and compliance requirements.

Supported Environments

The service supports recovery of workloads hosted across private, public, and hybrid environments. Supported platforms and recovery architectures are agreed during onboarding and documented in customer-specific service documentation.

Security and Data Protection

Security is embedded throughout the service design and operation.

The service includes:

- Secure, segregated recovery environments
- Encryption of data in transit and at rest
- Role-based access control and least-privilege principles
- Controlled access during recovery invocation
- Operational monitoring during recovery events

Centerprise operates an ISO-aligned Information Security Management System and applies consistent security controls across all managed cloud services.

Service Responsibility Model

Centerprise responsibilities:

- Operation and management of the DRaaS platform
- Provision and operation of UK-sovereign recovery infrastructure
- Recovery orchestration and technical execution
- Support during recovery invocation and testing
- Incident coordination and escalation

- Secure service exit and data handling

Customer responsibilities:

- Declaration of disaster recovery invocation
- Definition of recovery priorities and dependencies
- Validation of recovered services
- Business continuity planning outside the DRaaS platform

Service Management and Support

Support is provided through Centerprise's UK-based Service Desk, with access to specialist recovery engineers during recovery events.

Support includes:

- Incident handling and recovery coordination
- Invocation support during declared events
- Planned recovery testing and rehearsals
- Escalation and major incident management
- Service reporting as agreed

Onboarding and Transition

Structured onboarding ensures recovery readiness before the service is relied upon.

Onboarding typically includes:

- Definition of recovery scope and objectives
- Configuration of recovery environments
- Documentation of recovery procedures
- Validation through recovery testing
- Operational handover

The onboarding process aligns with customer governance, risk, and change processes.

Service Constraints and Dependencies

Recovery performance depends on the agreed recovery architecture, workload size, network connectivity, and recovery priorities.

The service requires up-to-date backup data and accurate recovery documentation. Invocation requires a customer declaration of a recovery event unless otherwise agreed.

Exit and Service Termination

Centerprise supports a secure and controlled service exit.

On exit:

- Recovery environments are decommissioned securely
- Residual customer data is deleted in line with agreed requirements
- Access is revoked following confirmation

Exit activities are planned to maintain security and compliance throughout offboarding.

Relationship to Other G-Cloud Services

This service builds upon Centerprise Backup as a Service delivered under G-Cloud Lot 3. The underlying sovereign infrastructure components are described separately in G-Cloud Lot 1.

Summary

Centerprise Disaster Recovery as a Service provides managed, secure, and assured recovery capability using UK sovereign infrastructure. By combining orchestrated recovery, strong security controls, and specialist operational support, the service enables organisations to meet business continuity and public sector assurance requirements.