# Business Cloud

# RTO, Disaster Recovery & Business Continuity Plan

### Applies to Business Cloud Plans S, M, and L

**Version:** RDB-2026.1

**Effective Date:** 12.01.2026

**Issued by:** Hub Hosting

**Contact:** sales@hub-hosting.com

## 1. Overview

This document outlines the Recovery Time Objective (RTO), Disaster Recovery (DR) plan, and Business Continuity Strategy (BCS) for the Business Cloud offerings (S, M, and L). All Business Cloud plans share the same managed infrastructure, security posture, and backup architecture, and differ only in allocated compute and storage resources.

These services are designed to support business-critical applications, ensure compliance with applicable regulations, and maintain operational continuity during technical incidents or disruptions.

## 2. Infrastructure and Service Capabilities

All Business Cloud plans include the following features:

- Fully Managed Environment
- Dedicated Resources:
  - Business Cloud S: 4 CPU, 16 GB RAM, 160 GB NVMe
  - Business Cloud M: 8 CPU, 32 GB RAM, 240 GB NVMe
  - Business Cloud L: 16 CPU, 64 GB RAM, 360 GB NVMe
- RAID-10 NVMe SSD Storage
- 10 Gbit/s Redundant Networking
- Cloud-based DNS with Full Administration
- SLA: 99.99% Uptime Guarantee
- Security Controls:
  - SSL Certificate
  - DDoS Protection
  - Web Application Firewall (WAF)
  - Intrusion Detection and Prevention (IDS/IPS)
  - Antivirus and Malware Protection
  - Brute-force Protection
  - SIEM and Monitoring
- Backup Architecture:

  - Daily full image backups stored within the same data center infrastructure (across multiple physical locations)
  - Hourly database backups stored on a remote offsite server
  - Weekly and monthly backups retained on remote storage
- Restore Timeframes:
  - System image: 10-15 minutes
  - Database: up to 20 minutes (depending on size)
  - Email services: 10-15 minutes
- 24/7 Technical Support

**3. Recovery Time Objective (RTO)**

**Defined RTO for all Business Cloud plans: ≤ 20 minutes**

The recovery time objective (RTO) reflects the maximum acceptable downtime following an incident. Due to a combination of automated restore procedures, optimized backup architecture, and administrative control over DNS, full system recovery can be achieved within 20 minutes under standard conditions.

System images can be restored within 10-15 minutes to alternate physical infrastructure within the same data center (multi-location).

Hourly database backups allow data recovery with minimal loss (Recovery Point Objective- RPO ≈ 1 hour).

Cloud DNS enables immediate rerouting of services to the newly restored instance, handled directly by the client or administrator.

Restore procedures are supported 24/7 with technical escalation paths.

**4. Disaster Recovery Plan (DRP)**

The Disaster Recovery Plan ensures the integrity and availability of services in the event of major system failure, hardware faults, cyberattacks, or localized outages.

**4.1 Disaster Recovery Components**

| Component | Description |
|---|---|
| **Backup Storage** | - Image backups within the same data center infrastructure (multi-location)<br>- Hourly DB backups to offsite server<br>- Weekly/monthly backups to remote storage |
| **Restore Procedures** | - System image restore: 10-15 min<br>- Database restore: up to 20 min |
| **Failover Capability** | - Restore supported across separate physical locations within the same data center provider infrastructure (intra-DC failover) |

| | | |
|---|---|---|
| | - | Not applicable across data centers or providers |
| **Cloud DNS Control** | - | Administrative access allows immediate DNS record changes to redirect traffic |
| **Redundant Networking** | - | 10 Gbit/s network with high availability across physical DC locations |
| **DR Testing** | - | Performed quarterly, including restore simulations and DNS rerouting drills |

**Note:** Failover is supported exclusively within the provider's infrastructure and physical boundaries of the same data center.

### 5. Business Continuity Strategy (BCS)

The Business Continuity Strategy ensures uninterrupted access to essential services and systems during adverse events, minimizing operational impact and service disruption.

#### 5.1 Key BCS Measures

- **Uptime Guarantee:** 99.99% SLA-backed availability across all Business Cloud plans
- **24/7 Support:** Continuous monitoring and incident response
- **Cloud DNS Management:** Administrative control ensures immediate rerouting during failover
- **Intra-DC Failover:** Image backups can be restored to alternate physical locations within the same data center, maintaining continuity in the event of localized failure
- **Proactive Monitoring:** SIEM systems detect anomalies and trigger early response mechanisms
- **Automated Restore Tools:** Ensure minimal human intervention in recovery processes
- **Compliance Alignment:** Supports operational resilience requirements under GDPR, NIS2, and related frameworks

### 6. Compliance Readiness

| Standard / Regulation | Status | Notes |
|---|---|---|
| **GDPR** | ✓ | Technical and organizational controls for personal data protection |
| **NIS2 Directive** | ✓ | Infrastructure supports availability, integrity, and resilience goals |
| **CMMC 2.0 - Level 2 Ready** | ✓ | Aligned with technical controls from NIST SP 800-171 (client must implement org. controls) |
| **NIST SP 800-171 / 800-53B** | ✓ | Security and privacy controls technically implemented (e.g. AC, AU, IR, SC, SI) |

| | | |
|---|---|---|
| **DISA STIG** | ✓ | Configurations can be aligned with STIG guidance upon request |

**7. Summary**

All Business Cloud plans (S, M, L) are equipped with robust backup mechanisms, advanced threat protection, and intra-datacenter failover capabilities. Recovery procedures, enabled by high-speed storage and cloud DNS management, allow full service restoration within ≤ 20 minutes in the event of an incident.

While cross-datacenter disaster recovery is not included by default, the architecture ensures high operational resilience within the same data center, leveraging redundant physical infrastructure and administrative DNS control for seamless failover.

## Standards and Regulations Supported by the Business Cloud Environment

| Standard / Regulation | Standard / Regulation | Notes |
|---|---|---|
| GDPR (General Data Protection Regulation) | ✅ Yes | Technical data protection measures implemented: encryption, access control, backup, audit logs |
| NIS2 (EU Directive on Security of Network and Information Systems) | ✅ Yes | High availability (SLA 99.99%), redundancy, incident response capabilities, SIEM integrated |
| CMMC 2.0 – Level 2 Ready | ✅ Yes | Technically aligned with NIST SP 800-171; organizational controls remain the responsibility of the client |
| NIST SP 800-171 Rev. 2 | ✅ Yes (technical) | Controls for protection of Controlled Unclassified Information (CUI): Access Control, Audit, System & Information Integrity, Media Protection, etc. |
| NIST SP 800-53B (Moderate Baseline) | ✅ Yes (technical) | Key security controls implemented (AC, AU, SC, IR, SI, CP, etc.) |
| ISO/IEC 27001:2022 (Information Security Management System) | ✅ Partial | Technical requirements supported; full compliance depends on the client's ISMS implementation |
| ISO/IEC 27017 (Cloud Security Controls) | ✅ Partial | Aligned with cloud security best practices |
| ISO/IEC 27018 (Protection of Personal Data in the Cloud) | ✅ Partial | Supports personal data protection in cloud environments |
| DISA STIG (Security Technical Implementation Guides) | ✅ Configurable | Instance can be configured according to STIG recommendations upon request |
| PCI DSS v4.0 (Payment Card Industry Data Security Standard) | ✅ Partial / Supported | Technical capabilities available; full compliance depends on client-side application and configuration |
| HIPAA (Health Insurance Portability and Accountability Act) | ✅ Partial / Supported | Technical safeguards for ePHI are supported; full compliance is client's responsibility |
| ITIL v4 (Service Management Best Practices) | ✅ Supported | Service environment and operational support aligned with ITIL principles (Incident, Change, Availability Management) |

### Clarifications:

| | |
|---|---|
| ✅ Yes | Technical and procedural controls are directly implemented in the instance infrastructure. |
| ✅ Partial / Supported | The infrastructure supports the technical requirements, but full compliance depends on the client's implementation (e.g. policies, data governance, documentation). |
| ✅ Configurable | The instance can be specifically configured to meet the given standard upon client request (e.g. DISA STIG alignment). |