TECHNOPEAK

Sample Disaster Recovery Plan

Prepared in TechnoPeak style for a fictional regulated finance client

Illustrative sample for landing-page and proposal use. This example is written in a regulator-aware, plain-language format and should be tailored during delivery to a real client environment, control set, and operating model.

Client	Crescent Capital Advisory LLC
Industry	Regulated financial services
Document type	Disaster Recovery Plan (DRP)
Version	1.0
Status	Sample / Illustrative
Review cycle	At least annually and after significant infrastructure change
Document owner	Technology & Operations
Prepared by	TechnoPeak

Prepared by TechnoPeak

Business continuity, disaster recovery, managed IT, and operational resilience advisory.

How this sample is positioned

This DRP is written as a cloud-first recovery document for a small regulated finance company. It is designed to look credible for board, compliance, and prospect-facing review while remaining practical and readable.

1. Purpose

This Disaster Recovery Plan defines the process for restoring critical IT services and supporting infrastructure after a serious disruption. It covers the technical actions needed to recover key systems, minimize downtime and data loss, and support continuity of regulated operations.

The DRP addresses technical restoration. Business workarounds, operational communication, and broader continuity decisions are addressed in the separate Business Continuity Plan.

2. Scope

This plan applies to user devices, Microsoft 365 services, identity access, internet and firewall services, document repositories, cloud-hosted line-of-business applications, telephony dependencies, security controls, and backup and restore processes that support the client's operating model.

- ransomware or destructive malware
- major endpoint compromise
- identity platform disruption
- critical data deletion or corruption
- firewall or internet edge failure
- cloud service outage
- hardware failure affecting office connectivity
- accidental misconfiguration causing service interruption

3. Recovery Strategy Overview

Crescent Capital Advisory LLC operates a cloud-first environment with limited on-site infrastructure. The recovery model prioritizes restoration of identity and communications, safe remote working capability, recovery from tested backups or vendor-supported restore options, and staged restoration based on business criticality rather than rebuilding everything at once.

4. Recovery Objectives

The following targets are illustrative and should be confirmed during onboarding, backup review, business impact analysis, and recovery testing. They are intended to demonstrate how TechnoPeak would package recovery tolerances in a deliverable suitable for a small regulated client.

System / Service	Priority	RTO	RPO
Microsoft 365 email and identity access	1	4 hours	1 hour to provider capability / last recoverable state
Secure remote access and MFA access path	1	4 hours	Minimal configuration loss
Client document repository	1	8 hours	4 hours

Core cloud line-of-business application	1	8 hours	4 hours or provider-supported restore point
Internet and firewall edge service	1	4 hours	Configuration restore from last backup
Telephony and key contact channels	2	8 hours	Not applicable
Internal shared working data	2	1 business day	8 hours
Non-critical internal systems	3	2 to 5 business days	1 business day

5. Roles and Responsibilities

Role	Responsibility
Recovery Manager - TechnoPeak Service Manager	Leads the technical recovery process, assigns resources, records milestones, and updates management during restoration.
Client Incident Sponsor - COO or CEO	Approves major recovery decisions, vendor escalation, spending, and business priority changes.
Identity and Productivity Lead - TechnoPeak Cloud Engineer	Handles Microsoft 365, Entra ID, MFA, mailbox access, Teams recovery, and user productivity restoration.
Network and Security Lead - TechnoPeak Infrastructure Engineer	Handles firewall, internet edge, remote access, device containment, and secure access validation.
Application Coordinator - Client owner with vendor support	Coordinates recovery of the core business application and confirms business validation after restoration.
Compliance Representative - Head of Compliance	Confirms evidence retention, reporting implications, and conditions for safely returning systems to service.

6. Recovery Preconditions

- incident scope has been identified as far as reasonably possible
- containment or isolation actions are completed where required
- decision made on restore versus rebuild
- backups or restore points have been verified
- vendor support tickets have been opened
- privileged access and recovery documentation are available
- key stakeholders are reachable and an incident bridge is active
- all actions and approvals are being logged

In a cyber event, recovery should not begin until containment is understood well enough to avoid reintroducing the issue into restored systems.

7. Technical Environment Summary

- Microsoft 365 productivity environment
- Entra ID with MFA enforcement
- SharePoint and OneDrive for document storage

- Teams for collaboration and meetings
- cloud-based regulated business application managed by third-party vendor
- managed office firewall and ISP connectivity
- corporate laptops with endpoint protection and disk encryption
- backup solution covering Microsoft 365 data and key configurations
- secure documentation repository for administrative records and recovery references

8. Backup and Recovery Controls

- daily backup of critical cloud data
- retention aligned to business and compliance requirements
- periodic restore testing rather than backup success assumption only
- export or backup of firewall configuration
- secure storage of recovery credentials and emergency procedures
- documented administrative contacts for cloud, telecom, application, and backup providers
- protected copies of inventories, architecture notes, and support contacts
- immutable or otherwise protected backup strategy where feasible

9. Recovery Triggers

- outage exceeds the accepted service threshold for a critical system
- data loss or corruption affects priority records
- ransomware is confirmed or strongly suspected
- primary working method is unavailable and cannot be restored quickly
- management declares disaster recovery mode
- third-party outage materially affects critical service delivery

10. Recovery Sequence

10.1 Phase 1 - Triage and containment

1. Confirm incident type and scope.
2. Isolate affected devices, accounts, or network segments.
3. Preserve logs and evidence where needed.
4. Disable compromised accounts if required.
5. Escalate to vendors and management.

10.2 Phase 2 - Establish core access

1. Restore identity platform access.
2. Validate admin account integrity.
3. Confirm MFA functionality.
4. Re-establish secure communications.
5. Ensure recovery team access to documentation and consoles.

10.3 Phase 3 - Restore critical services

1. Microsoft 365 identity and email.
2. Remote access path and secure endpoint posture.

3. Document repository and regulated records access.
4. Core cloud line-of-business application.
5. Internet and office network services.
6. Telephony and secondary services.

10.4 Phase 4 - Validate and return to service

1. Confirm system integrity and expected functionality.
2. Obtain business-owner validation.
3. Re-enable and verify security controls.
4. Retire temporary workarounds.
5. Inform users of restored service status.
6. Increase monitoring for the immediate post-recovery period.

11. Recovery Procedures by Service

Microsoft 365 / Identity access

- verify whether the issue is provider-side or tenant-side
- validate admin access and privileged account integrity
- review conditional access, MFA, and sign-in failures
- restore deleted or corrupted objects if applicable
- verify mailbox access for key users and Teams communication

Success criteria: key staff can authenticate securely, send and receive email, and access Teams and essential files.

Document repository

- determine whether the issue is deletion, corruption, permission drift, sync error, or wider outage
- restore affected files, folders, or libraries from the approved recovery source
- verify access permissions and confirm no inappropriate exposure has been introduced
- validate required document availability with business and compliance owners

Success criteria: client servicing teams and compliance can access required current records.

Core business application

- contact the application vendor and invoke priority support
- establish whether the issue is application, identity, connectivity, or data related
- execute the vendor-supported restoration process
- validate user access and critical workflows before return to production

Success criteria: designated users can access the system and complete core business processes.

Firewall / network / internet edge

- assess whether the cause is hardware failure, configuration error, ISP outage, or security event
- switch to backup configuration or replacement unit if needed
- restore saved configuration and validate internet, DNS, and traffic rules
- confirm remote access and endpoint communications

Success criteria: office and remote users can reach approved services securely.

Endpoint recovery

- isolate affected devices
- wipe and rebuild where compromise is suspected
- re-enroll devices in the management platform and redeploy security controls
- restore approved user data and validate sign-in and application access

Success criteria: recovered devices are clean, compliant, and functional.

12. Cyber Recovery Considerations

- containment comes before restoration
- privileged accounts are reset where compromise is suspected
- indicators of compromise are reviewed before reconnecting systems
- rebuild is preferred over partial cleanup for materially affected endpoints where risk is elevated
- backup integrity is verified before any restore is accepted as complete
- management retains ownership of legal, regulatory, and client communication decisions

13. Vendor and Third-Party Dependencies

Key dependencies include Microsoft, the internet service provider, telephony provider, cloud business application vendor, backup provider, endpoint security vendor, and facilities provider for office access. For each critical dependency the client should maintain support contacts, account identifiers, escalation paths, expected response times, and known workaround procedures.

14. Communication During Recovery

- update management at incident declaration
- issue technical status after triage
- communicate at each major restoration milestone
- confirm service restoration and post-recovery monitoring status
- close with final incident summary and lessons learned

Updates should include systems affected, business impact, actions taken, recovery stage, key risks, open dependencies, and any management decisions still required.

15. Testing and Validation

- tabletop exercises for management and technical leads
- backup restore tests
- Microsoft 365 recovery validation
- firewall configuration restore validation
- endpoint rebuild and re-enrollment test
- vendor escalation drill for critical SaaS dependency
- post-change review after major infrastructure changes

A test is only considered meaningful when the restore was actually performed or credibly simulated, timings were recorded, issues were logged, and corrective actions were assigned.

16. Plan Maintenance

- new critical systems are introduced
- backup platform or retention model changes
- identity, network, or remote-access architecture changes
- office location or operating model changes
- new regulatory expectations or client recovery commitments arise
- tests or live incidents reveal control gaps

17. Approval

Approved by: Omar Siddiqui, Chief Operating Officer, Crescent Capital Advisory LLC

Prepared and supported by: TechnoPeak - IT Resilience, Recovery, and Managed Services