TECHNOPEAK

Sample Business Continuity 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	Business Continuity Plan (BCP)
Version	1.0
Status	Sample / Illustrative
Review cycle	Annual and after any major operational or technology change
Document owner	Chief Operating Officer
Prepared by	TechnoPeak

Prepared by TechnoPeak

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

Purpose of this sample

This document demonstrates how TechnoPeak can package a continuity deliverable for a small regulated firm: practical, structured, readable, and suitable for review by management, auditors, and compliance stakeholders.

1. Purpose

This Business Continuity Plan defines how Crescent Capital Advisory LLC will continue to deliver its critical services during and after a disruptive event. The focus of this plan is business continuity: how the firm keeps operating when normal working conditions are interrupted.

The objectives of this plan are to protect people, maintain client and regulatory communication, preserve access to critical records, support timely decision-making, and provide an organized framework for operating through disruption until normal conditions are restored.

2. Scope

This plan applies to the firm's primary office, all permanent employees and critical contractors, end-user devices, Microsoft 365 services, telephony, internet connectivity, cloud applications used for regulated operations, and key third-party dependencies.

- office inaccessibility or building emergency
- power failure, internet outage, or telecom disruption
- cyber incident affecting normal business operations
- cloud service outage or vendor-side disruption
- critical employee unavailability
- major IT service interruption
- third-party supplier failure

3. Business Overview

Crescent Capital Advisory LLC is a small regulated financial advisory firm operating from a single Dubai office with 28 employees. The business relies on Microsoft 365 for email, collaboration, and document handling; cloud-based line-of-business applications for case and record management; corporate laptops for all employees; a managed firewall and secure remote access; and outsourced IT support and resilience services provided by TechnoPeak.

The continuity model for the firm is remote-first, which means the business is expected to continue operating through most short- to medium-duration disruptions using approved laptops, multi-factor authentication, cloud services, mobile connectivity, and a defined management escalation process.

4. Continuity Objectives

1. Preserve life and safety and account for all personnel during any major disruption.
2. Maintain communication with staff, clients, regulators, and critical suppliers.
3. Continue or restore priority business activities within acceptable timelines.
4. Protect confidential, client, and regulated information at all times.
5. Minimize operational, compliance, reputational, and financial impact.
6. Record decisions, escalation points, and temporary workaround measures clearly.
7. Restore normal operations in a controlled and well-documented manner.

5. Governance and Responsibilities

Role	Responsibility
Incident Director - Chief Executive Officer	Responsible for major business decisions, approval of regulatory communication, and overall direction during a disruption.
Business Continuity Lead - Chief Operating Officer	Coordinates plan activation, maintains the incident log, tracks business impact, assigns workarounds, and manages recovery priorities.
Technology Recovery Lead - TechnoPeak Service Manager	Coordinates technical assessment and restoration activities in line with the Disaster Recovery Plan and technical escalation procedures.
Compliance Lead - Head of Compliance	Assesses reporting obligations, records control expectations, client notification requirements, and regulatory implications.
People Lead - HR / Administration Manager	Supports staff welfare, attendance confirmation, alternate work location needs, and internal staff coordination.
Communications Lead - Office Manager or delegate	Issues approved internal and external communications to stakeholders using agreed channels.

The Business Continuity Plan may be invoked by the Chief Executive Officer, Chief Operating Officer, Head of Compliance, or TechnoPeak escalation contact where immediate action is required and firm approvers are unavailable.

6. Critical Business Services

Critical services are grouped according to how quickly they must be maintained or restored. This reflects the firm's business impact analysis and the practical tolerance for short disruption within a small regulated operating model.

Priority 1 - Urgent services

- client communications and management oversight
- access to Microsoft 365 email and Teams
- access to client records and regulated documentation
- compliance decision-making and incident reporting capability
- secure remote working capability for key staff

Target tolerance: same business day to four hours for core communications, and up to eight hours for stabilized operating mode across critical teams.

Priority 2 - Important services

- internal reporting
- general administration
- finance and procurement processing
- non-urgent client preparation work

Target tolerance: one to two business days.

Priority 3 - Deferrable services

- long-term internal improvement work
- non-urgent archiving and housekeeping
- lower-priority maintenance tasks

Target tolerance: up to five business days.

7. Minimum Resource Requirements

- current employee and vendor contact list
- Microsoft 365 email and Teams availability
- secure endpoint devices and MFA
- internet connectivity or mobile-data alternative
- access to essential client and compliance records
- availability of management approvers and deputies
- conference bridge or alternate communication method
- alternate work location or remote work readiness

8. Disruption Scenarios and Response Actions

Office inaccessible

Examples include building evacuation, fire alarm, water leak, physical security concern, or facilities failure. The firm will shift to remote work, issue staff instructions within 30 minutes, confirm device and MFA access, and prioritize client-facing and compliance staff for immediate activation.

Internet or telecom outage

The firm will fail over to mobile hotspot or secondary connectivity where available, move urgent communication to mobile and Teams, log a provider incident reference, and relocate selected staff to an alternate location if the outage exceeds two hours.

Microsoft 365 or cloud service disruption

The firm will verify whether the issue is local, tenant-level, or provider-side, move to alternate communication methods, use approved offline contact lists where needed, and postpone non-essential processing until service is restored.

Cyber incident or suspected ransomware

Affected devices will be isolated immediately, use of impacted systems will be suspended, the incident team will convene without delay, and recovery will proceed together with the Disaster Recovery Plan and incident response process.

Critical staff unavailability

Deputy coverage will be activated, approvals reassigned to designated alternates, and client responsibilities redistributed. Non-critical work will be deferred until staffing stabilizes.

Third-party provider failure

The firm will escalate to the relevant supplier, establish expected duration and workaround options, switch to manual methods where available, and assess whether regulated activities are materially impacted.

9. Workaround Arrangements

- remote work from home using business laptops
- Teams or mobile calling in place of office telephony
- temporary manual approval using documented emergency authority
- secure use of pre-approved templates and working copies where policy permits
- alternate assignment of staff for essential client communication
- offline emergency contact register maintained by management

All workarounds are temporary. Any deviation from standard process must be documented and reconciled once normal service is restored.

10. Communication Plan

10.1 Internal communication

Primary channels are Microsoft Teams, email, and phone. If these are unavailable, the firm will use an emergency messaging tree. The first internal update should confirm the nature of the disruption, whether the BCP is activated, what staff should do immediately, which services are affected, and when the next update will be provided.

10.2 External communication

External communication may be required with clients, regulators, auditors, insurers, and key suppliers. Only approved representatives may issue external statements: the Chief Executive Officer, Chief Operating Officer, Head of Compliance, or a delegated spokesperson formally authorized by management.

11. Alternate Workplace Strategy

The primary continuity strategy is remote-first operation. All permanent staff are issued business laptops, MFA is enabled for corporate access, and key managers can work remotely on short notice. Where needed, selected leadership and client-facing personnel may be directed to an alternate serviced office arrangement for short-term coordination or high-priority meetings.

12. Incident Logging and Decision Tracking

- time of disruption and how it was identified
- services affected and business impact observed
- decisions made and who approved them
- communications issued internally and externally
- assigned actions, owners, and target completion times
- restoration milestones and final closure date
- lessons learned and corrective actions

13. Plan Activation and Recovery Stages

1. Assess: identify affected services, confirm staff safety, estimate outage duration, and decide whether to invoke the plan.
2. Stabilize: activate the incident team, issue instructions, implement workarounds, and prioritize critical operations.
3. Operate in continuity mode: continue Priority 1 activities, monitor impact, escalate risk, and track resource gaps.
4. Restore normal operations: confirm technical restoration, retire workarounds in a controlled manner, and reconcile temporary records.
5. Review: hold a post-incident review, record lessons learned, and update the BCP, DRP, and contact lists where needed.

14. Training, Testing, and Maintenance

- annual continuity awareness briefing for all employees
- annual tabletop exercise involving management and TechnoPeak
- periodic remote work readiness and contact list checks
- review after major business, technology, office, or supplier change
- post-incident update where a real event reveals plan gaps

15. Review Triggers

- major business or regulatory change
- change of office, operating model, or outsourcing arrangement
- change to critical systems or supplier landscape
- serious incident or audit finding
- scheduled annual review date

16. Approval

Approved by: Aisha Rahman, Chief Executive Officer, Crescent Capital Advisory LLC

Supported by: TechnoPeak - Business Continuity and IT Resilience Advisory