



Business Continuity Planning (BCP)

A project-based approach to design, implement, and operationalize BCP for mid-sized consulting & services organizations.

PUBLISHED BY

Levrara Consulting Group

Index Summary

- | | |
|----|---|
| 01 | Purpose, Objectives, and Success Criteria |
| 02 | Scope and Boundaries |
| 03 | Stakeholders, Roles, and RACI |
| 04 | BCP vs DR vs Incident Management vs Crisis Management |
| 05 | Typical Disruption Scenarios |
| 06 | Delivered BCP Framework (Mapped Process Groups) |
| 07 | Work Breakdown Structure (WBS) - High-Level |
| 08 | High-Level Schedule (30-60-90 Day Roadmap) |
| 09 | Communications Management () |
| 10 | Risk, Issue, and Dependency Management (RAID) |
| 11 | Testing, Rehearsal, and Quality Management |
| 12 | Recommendations for Mid-Sized Consulting / Services Organizations |
| 13 | Conclusion |
| 14 | Annexures (Templates) |

Executive Summary

Business Continuity Planning (BCP) is an enterprise resilience capability that ensures continuation of critical services during disruptions. This paper presents BCP not only as a policy or compliance activity, but as a structured program delivered using project management practices ensuring scope clarity, stakeholder alignment, measurable outcomes, governance, and continuous improvement.

The whitepaper provides a practical BCP framework suitable for Levrara Consulting Group (a mid-sized consulting & services organization), including Business Impact Analysis (BIA), criticality and dependency mapping, recovery objectives (RTO/RPO), continuity strategies across people/process/technology/vendors, governance, and testing.

Key outcomes include:

- Repeatable BCP lifecycle mapped to process groups (Initiate, Plan, Execute, Monitor & Control, Close)
- Defined ownership and governance model with measurable success criteria
- Practical templates (BIA, RTO/RPO matrix, communication tree, vendor criticality checklist, RAID log, change control) to accelerate implementation and client conversations

This first draft is designed to be client-ready in tone and structure and can be refined further based on organizational context, systems landscape, and target maturity.

Levrara Context and Operating Model Assumptions

This whitepaper is written to be directly usable for Levrara client conversations and internal delivery readiness. The following assumptions reflect a typical consulting and services operating model and can be adjusted during iteration:

Project-based client engagements with defined SLAs, delivery milestones, and reputational impact from service disruption.

Distributed teams (multi-location / remote) dependent on identity access, connectivity, collaboration tools, and client environments.

Time-bound operational obligations such as timesheets, invoicing, payroll processing, and statutory/regulatory commitments.

Resource allocation and staffing (including rapid replacement of key personnel) as a core continuity dependency.

Third-party and SaaS reliance (payroll, HR, finance, ticketing, cloud platforms) plus client-mandated tools and access constraints.

Client onboarding and compliance activities (e.g., background verification / BGV) that can block delivery if disrupted.

Purpose, Objectives, and Success Criteria

1.1 Purpose

Establish an organization wide BCP capability to maintain or rapidly resume critical services during disruptive events, protecting revenue, client commitments, compliance obligations, and reputation.

1.2 Objectives

- Identify critical processes and dependencies via BIA for priority services.
- Define recovery objectives (RTO/RPO) and minimum service levels for critical processes.
- Implement continuity strategies and documented plans for priority services (Tier 1).
- Establish governance, roles, communications, and a test cadence for ongoing readiness.

1.3 Success Criteria (Acceptance Metrics)

BIA coverage:

>90% of Tier 1 processes completed and approved by process owners.

Critical role resilience:

100% of Tier 1 roles have named backups and documented runbooks.

Exercise readiness:

At least 1 tabletop exercise and 1 functional drill completed for Tier 1 scenarios.

Formal Sign-Off

From Business Owners, IT Owners, and Risk/Compliance on scope, tiers, and recovery targets.

Scope and Boundaries

In Scope

- Business Impact Analysis (BIA), process criticality, and dependency mapping.
- Definition of recovery objectives (RTO/RPO) and tiering model.
- Continuity strategies across people, process, technology, vendors, and facilities.
- Governance model (RACI), escalation and communications framework, and operating rhythm.
- Testing and rehearsal plan with KPIs and continuous improvement backlog.

Assumptions and Constraints

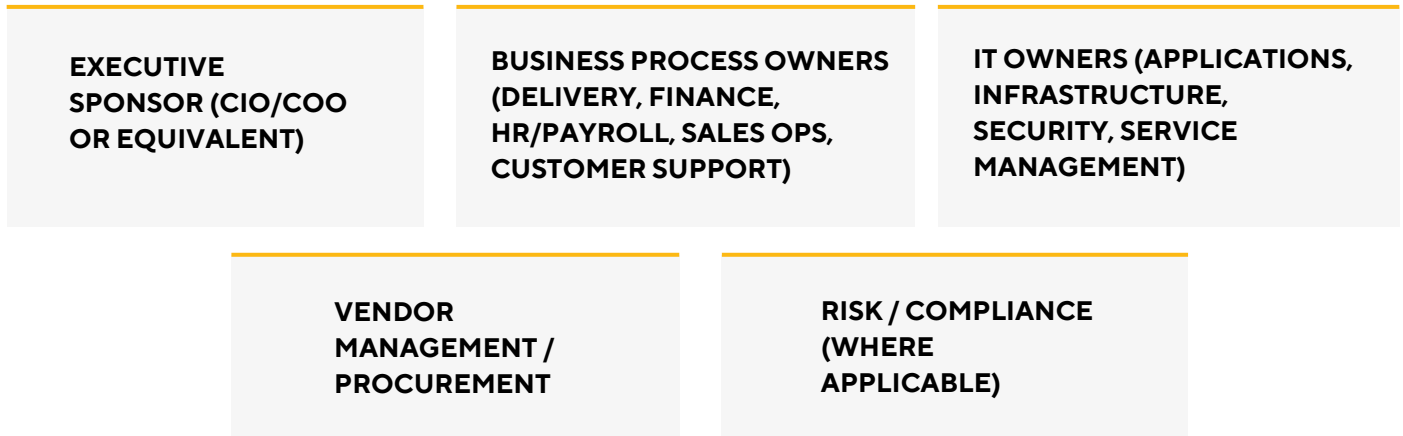
- Availability of business process owners for BIA workshops and plan validation sessions.
- Access to application and infrastructure inventories and architectural inputs for dependency mapping.
- Timely availability of vendor continuity evidence (SLA/BCP summaries, test attestations).
- This document is a first draft delivered under an accelerated timeline; annexures are provided as practical V1 templates.

Out of Scope (Initial Phase)

- Major platform re-architecture or modernization (unless required as part of an approved continuity strategy).
- Deep technical DR engineering for all systems (managed as separate IT projects/workstreams).
- Full enterprise-wide rollout across all geographies in a single phase (recommended: phased deployment starting with Tier 1).

Stakeholders, Roles & RACI

3.1 Key Stakeholders



3.2 RACI Matrix

ACTIVITY	SPONSOR	BCP LEAD	BUSINESS OWNER	IT OWNER	VENDOR / RISK
Approve scope & tiers	A	R	C	C	C
Conduct BIA workshops	C	R	A	C	C
Define RTO / RPO	C	R	A	A	C
Define continuity strategies	C	R	A	A	C
Approve plans	A	R	A	A	C
Execute tests & lessons learned	C	R	A	A	C

Legend: R = Responsible, A = Accountable, C = Consulted.

BCP vs DR vs Incident vs Crisis Management

BCP is often confused with other resilience disciplines. The following view clarifies differences and how they link together.

MINUTES-HOURS Incident Management Owner: IT Ops / Service Management Primary objective: Restore service quickly. Focus Area: Detection, triage, fix, restore	HOURS-DAYS Disaster Recovery (DR) Owner: IT Infrastructure / Apps Primary objective: Recover IT systems and data. Focus Area: Failover, restore, RTO/RPO delivery
HOURS-WEEKS Business Continuity (BCP) Owner: Business (IT as enable) Primary objective: Continue critical business services. Focus Area: Process continuity, minimum viable operations	IMMEDIATE-ONGOING Crisis Management Owner: Executive Leadership Primary objective: Protect people, brand, decisions. Focus Area: Governance, comms, stakeholder management

4.1 Linkages

These capabilities are complementary incidents may trigger BCP invocation when impact thresholds are exceeded DR enables technology recovery; crisis management provides decision authority and communications oversight BCP ensures business outcomes continue through predefined strategies and workarounds.

Typical Disruption Scenarios

A practical BCP for consulting/services operations should address the following disruption patterns:

5.1

Cyber Disruptions

- Ransomware causing system unavailability and data integrity concerns
- Identity compromise affecting access to delivery tools and client data
- Third-party breach impacting shared platforms or integrations

5.2

Technology & Infrastructure Disruptions

- Cloud region or major SaaS outage
- Network/connectivity failure affecting remote delivery
- Data corruption or failed release/deployment

5.3

People & Capability Disruptions

- Key-person dependency in specialized delivery/administration roles
- Sudden unavailability of critical staff due to health events or attrition
- Delivery capacity constraints during peak periods

5.4

Vendor & Third-Party Disruptions

- Payroll vendor outage impacting salary processing and compliance obligations
- Outsourced service provider failure (IT managed services, finance ops)
- Vendor contractual or insolvency events

5.5

Facility & Regional Disruptions

- Office shutdown due to fire/flood/utility outage
- Regional events restricting access and movement

Delivered BCP Framework (Mapped Process Groups)

6.1 Initiation – BCP Charter

The BCP program should start with a clear charter that defines the business case, scope, tiers, key stakeholders, governance, and initial deliverables. The charter sets decision rights and ensures continuity is treated as a business capability, with IT as a key enabler.

6.2 Planning – Core BCP Design Deliverables

Planning produces the baseline design and artifacts required for effective execution:

- B1A plan, workshop schedule, and data collection approach.
- Process tiering model (Tier 1/2/3) and minimum service levels.
- Dependency mapping – people, applications, data, infrastructure, vendors, facilities.
- Recovery objectives (RTO/RPO) definitions and target ranges by tier.
- Continuity strategy catalog across people, process, technology, vendor, and facility dimensions.
- Communications plan – stakeholder updates, invocation criteria, message templates.
- Testing strategy and calendar

6.3 Execution – Build Continuity Capability

- Conduct B1A workshops with process owners and validate outcomes.
- Define and agree RTO/RPO targets and dependency maps.
- Develop continuity plans and runbooks, including minimum viable operations and manual workarounds.
- Assess vendor criticality and obtain continuity evidence for Tier 1 vendors.
- Establish communications tree and invocation procedures.

6.4 Monitoring and Controlling – Controls and Quality

- Scope and change control for RTO/RPO and strategy changes (via Steering Committee / CCB).
- Quality reviews and approvals of B1A outputs and continuity plans.
- KPI dashboard: plan coverage, exercise completion, action closure, vendor assurance status.
- RAID log management (Risks, Assumptions, Issues, Dependencies).

6.5 Closing – Formalize & Transition to BAU

- Lessons learned captured following initial exercise cycle
- Baseline plans approved and published; ownership confirmed
- Transition to a BAU governance rhythm (quarterly reviews, annual refresh, change triggers)

Work Breakdown Structure (WBS) - High-Level

- 1.0 INITIATE & GOVERN
- 2.0 BIA & PROCESS TIERING
- 3.0 DEPENDENCY MAPPING
- 4.0 RECOVERY OBJECTIVES (RTO/RPO)
- 5.0 CONTINUITY STRATEGIES
- 6.0 PLAN DEVELOPMENT (BCP DOCUMENTS + RUNBOOKS)
- 7.0 VENDOR RESILIENCE ASSURANCE
- 8.0 COMMUNICATIONS & CRISIS LINKAGE
- 9.0 TESTING & EXERCISE EXECUTION
- 10.0 REPORTING, IMPROVEMENTS & BAU TRANSITION

High-Level Schedule (30-60-90 Day Roadmap)

- 0-30 DAYS Discover & Design**
 - Confirm charter, scope, stakeholders, governance, and tiering approach.
 - Run BIA workshops for Tier 1 services (start with client delivery, payroll, finance).
 - Draft dependency maps and initial RTO/RPO proposals.
- 31-60 DAYS Build**
 - Finalize RTO/RPO targets and approve tiering outcomes.
 - Develop continuity plans and runbooks; define minimum viable operations.
 - Assess Tier 1 vendor criticality; collect and review vendor resilience evidence.
 - Create communications tree and invocation playbook.
- 61-90 DAYS Validate & Operationalize**
 - Conduct table-top exercises for top scenarios (cyber, SaaS outage, payroll disruption).
 - Execute functional drills for 1-2 critical processes; validate workarounds.
 - Capture lessons learned; create prioritized improvement backlog and BAU cadence.

Communications Management

A structured communications approach ensures stakeholder alignment and consistent messaging during disruptions.

9.1 Operating Updates

- Weekly working group: BCP lead, business owners, IT owners (progress, issues, dependencies).
- Monthly steering committee: decisions on scope, targets, strategy, and resourcing.
- Quarterly leadership updates: readiness posture, test outcomes, key risks.

9.2 Invocation communications

- Pre-approved message templates for internal stakeholders and clients (as applicable).
- Defined spokespersons and approval flow for external communications.
- Contact tree validation (quarterly).

Risk, Issue & Dependency Management (RAID)

RAID management provides visibility and control across the BCP program lifecycle. A RAID log template is included in Annexure E.

TYPE	EXAMPLE	MITIGATION/ ACTION
Risk	Vendor continuity evidence unavailable or outdated	Define evidence standards and timelines; escalate via procurement.
Risk	Unrealistic RTO/RPO targets not supported by current capability	Align targets to tiering and investment decisions.
Issue	Missing application/integration inventory;	Establish a baseline inventory as a dependency for dependency mapping.
Dependency	DR capability improvements required for Tier 1 systems	Initiate IT workstream with defined milestones.

Testing, Rehearsal, and Quality Management

11.1 Test types

- Tabletop exercises: scenario-based discussions to validate roles, decisions, and communications.
- Scenario walkthroughs (functional drills): validate process workarounds end-to-end.
- Technical DR tests: validate failover/restore and RTO/RPO feasibility.
- Crisis simulation: validate leadership decision-making and stakeholder management.

11.2 Suggested frequency (baseline)

- Tabletops for Tier 1 scenarios: 2-4 times per year.
- Contact tree validation: quarterly.
- DR technical tests for critical systems: at least annually (more frequent where risk/impact is high).
- Vendor resilience review: annually and after significant vendor incidents or changes.

Levrara-specific vendor assurance focus areas:

Payroll/HR platforms, finance systems, collaboration suite, identity provider, ticketing/service management tools, cloud platforms, and any client-mandated delivery platforms where continuity depends on client access.

11.3 Quality criteria (examples)

- BCP plan completeness checklist met (scope, triggers, roles, workarounds, dependencies, communications).
- Formal approvals recorded for BIA outputs and continuity plans.
- Exercise evidence captured (minutes, outcomes, actions) and action closure tracked.

Recommendations for Mid-Sized Consulting / Services Organizations

- Anchor continuity on client delivery and time-bound obligations (payroll, invoicing, statutory).
- Make BCP business-owned; ensure IT enables recovery but does not solely drive continuity decisions.
- Reduce key-person dependency through RACI, backups, cross-skilling, and runbooks.
- Treat SaaS and third parties as primary continuity risks; tier vendors and demand evidence.
- Define minimum viable operations for disruption periods; optimize for practicality.
- Prioritize exercises that validate real behavior (tabletops and walkthroughs) over document volume.

Conclusion

BCP is most effective when delivered as a managed program using disciplines ensuring stakeholder alignment, scope control, measurable outcomes, and continuous improvement. For consulting/services organizations, a pragmatic, vendor-inclusive, test-driven approach strengthens resilience while maintaining cost and delivery realism.

Annexures (Templates)

● Annexure A: Business Impact Analysis (BIA) Template

Use the following as a fillable template for each process or service undergoing BIA. One record per process/service owner.

FIELD	VALUE
Process / Service Name	
Process Owner	
Backup Owner	
Service Description / Outcome	
Criticality (High/Med/Low)	
Peak periods / cutoffs	
Impact categories (Revenue / SLA / Legal / Reputation)	
Impact over time (0-4h / 4-24h / 1-3d / 3-7d / >7d)	
MTPD/MTD	
Target RTO	
Target RPO (if data involved)	
Upstream dependencies	
Downstream dependencies	
Key applications	
Key infrastructure (network/identity/etc.)	
Key vendors / SaaS	
Key data repositories	
Manual workaround (Yes/No + steps)	
Minimum staffing / skills needed	
Approvals / decision authority	
Notes / assumptions	

● **Annexure B: RTO/RPO Matrix (Template)**

PROCESS / APP	TIER	RTO	RPO	NOTES

● **Annexure C: Communication Tree (Template)**

ROLE	NAME	BACKUP	PHONE	EMAIL	TRIGGER

● **Annexure D: Vendor Criticality Checklist (Template)**

CHECKLIST ITEM	YES/NO	EVIDENCE / NOTES
Vendor supports a critical business process		
Documented BCP/DR available		
Stated RTO/RPO meets business needs		
Recent test evidence available		
SLA uptime and support model defined		
Incident notification time defined		
Data backup, retention, and restore clarity		
Security posture evidence (audits/certifications)		
Exit strategy / alternative option exists		

● **Annexure E: RAID Log Template ()**

ID	TYPE	DESC	IMPACT	PROB	OWNER	ACTION	DUE	STATUS

● **Annexure F: Change Control Template ()**

ID	CHANGE	REASON	IMPACT	APPROVER	DECISION	DATE