Business Continuity FRAMEWORK

<Acme>: **Business Continuity Plan**

Project # FXXXX

Business Confidential Release 1.0

<Date>

A black background with blue letters

Description automatically generated

***Logo, company name

Description automatically generated***

Table of Contents

[Introduction 5](#_Toc171673256)

[Executive Summary 5](#_Toc171673257)

[Phase 1: Preparation and Training Phase (Technology and IT Continuity Focus) 7](#_Toc171673258)

[Roles and Responsibilities: 7](#_Toc171673259)

[Specific Roles and Responsibilities for Preparation and Training 7](#_Toc171673260)

[Process for Maintaining Business Impact Analysis (BIA), System Dependency, and Individual System Recovery Plans 8](#_Toc171673261)

[Process for Maintaining Contact Lists and Roles/Responsibilities for Business Continuity 9](#_Toc171673262)

[Training and Validation Exercises 10](#_Toc171673263)

[Tabletop Exercises 10](#_Toc171673264)

[Validation Exercises 11](#_Toc171673265)

[Schedule and Timing 12](#_Toc171673266)

[Preparation and Training - Estimated Level of Effort (LOE) by Role 12](#_Toc171673267)

[Preparation and Training – Yearly Calendar 13](#_Toc171673268)

[Phase 2: Activation and Notification Phase 14](#_Toc171673269)

[Specific Roles and Responsibilities for Activation and Notification 14](#_Toc171673270)

[Activation Criteria 14](#_Toc171673271)

[Notification Procedures 15](#_Toc171673272)

[Outage Assessment 16](#_Toc171673273)

[Schedule and Timing 17](#_Toc171673274)

[Activation and Notification routine tasks - Estimated Level of Effort (LOE) by role 17](#_Toc171673275)

[Activation and Notification – Yearly Calendar 17](#_Toc171673276)

[Phase 3: Recovery Phase 18](#_Toc171673277)

[Specific Roles and Responsibilities for the Recovery Phase: 18](#_Toc171673278)

[Recovery Process in Sequence: 18](#_Toc171673279)

[1. Safety and Security: 18](#_Toc171673280)

[2. Prioritize IT Recovery Tasks. 18](#_Toc171673281)

[3. Infrastructure Restoration 18](#_Toc171673282)

[4. Data Recovery 18](#_Toc171673283)

[5. IT Operations Restoration 19](#_Toc171673284)

[6. Testing and Validation 19](#_Toc171673285)

[7. Communication 19](#_Toc171673286)

[8. Continuous Monitoring 19](#_Toc171673287)

[Schedule and Timing 19](#_Toc171673288)

[Recovery Phase Tasks - Estimated Level of Effort (LOE) by Role 19](#_Toc171673289)

[Phase 4: Reconstitution Phase 20](#_Toc171673290)

[Concurrent Processing 20](#_Toc171673291)

[Parallel Operations 20](#_Toc171673292)

[Gradual Transition 20](#_Toc171673293)

[Testing 20](#_Toc171673294)

[Functional Testing: 20](#_Toc171673295)

[Integration Testing: 20](#_Toc171673296)

[Load Testing: 21](#_Toc171673297)

[Security Testing: 21](#_Toc171673298)

[Notifications 21](#_Toc171673299)

[Stakeholder Updates: 21](#_Toc171673300)

[Completion Announcement: 21](#_Toc171673301)

[Feedback Request: 21](#_Toc171673302)

[Cleanup 21](#_Toc171673303)

[Temporary Infrastructure: 21](#_Toc171673304)

[Data Cleanup: 22](#_Toc171673305)

[Resource Reallocation: 22](#_Toc171673306)

[Documentation 22](#_Toc171673307)

[Process Documentation: 22](#_Toc171673308)

[System Documentation: 22](#_Toc171673309)

[Lessons Learned: 22](#_Toc171673310)

[Policy Updates: 22](#_Toc171673311)

[Final Summary Report: 22](#_Toc171673312)

[Appendix A – Contact List 23](#_Toc171673313)

[Appendix B – Risks Considered 24](#_Toc171673314)

[Appendix C – Major Business Process to BU Map 25](#_Toc171673315)

[Appendix D – Business Process to Technology Map 29](#_Toc171673316)

[Appendix E – Technology RTO (BIA) 34](#_Toc171673317)

[Appendix F – Example Tabletop Exercise Outline 35](#_Toc171673318)

[Purpose 35](#_Toc171673319)

[Scenario 35](#_Toc171673320)

[Participants 35](#_Toc171673321)

[Exercise Phases 36](#_Toc171673322)

[1. Initial Briefing 36](#_Toc171673323)

[2. Scenario Presentation 36](#_Toc171673324)

[3. Recovery Phase Simulation 36](#_Toc171673325)

[4. Reconstitution Phase Simulation 37](#_Toc171673326)

[5. Debriefing and Evaluation 37](#_Toc171673327)

[Evaluation Criteria 38](#_Toc171673328)

[Final Grade 38](#_Toc171673329)

[Follow-up Actions 38](#_Toc171673330)

# Introduction

In today's rapidly evolving business environment, the ability to maintain operational continuity during and after unexpected disruptions is critical. This Business Continuity Plan (BCP) is designed to prepare our organization for unforeseen events that could jeopardize the stability and functionality of our technological infrastructure and overall business operations. This plan aims to ensure the resilience of our IT systems, safeguard critical data, and maintain essential business processes in the face of emergencies, thus minimizing downtime and ensuring a swift recovery.

This plan's scope is limited to ensuring the continuity of business operations in the face of technology interruption. The document's framework could be extended to other types of disaster planning, but that is beyond the scope of the current plan.

The Business Continuity Plan is structured into four main phases: *Preparation and Training*, *Activation and Notification*, *Recovery*, and *Reconstitution*. Each phase encompasses detailed procedures, roles, responsibilities, and protocols that collectively ensure a comprehensive response to any business interruption. This document outlines the necessary steps to prepare our personnel, systems, and infrastructure to respond effectively to potential threats, thereby enhancing our ability to recover and resume normal operations with minimal disruption.

# Executive Summary

The Business Continuity Plan (BCP) provides a robust framework for ensuring the continuous operation of our organization's critical business processes and IT systems. This plan, which borrows heavily from the NIST standard[[1]](#footnote-1), is re-sized for non-government entities in the small to medium enterprise category. Business Continuity planning is essential for maintaining business integrity and operational functionality during emergencies, such as system failures, cybersecurity incidents, natural disasters, and other unexpected disruptions. The BCP is divided into four key phases, each addressing specific continuity planning and response aspects:

| Phase | Purpose |
| --- | --- |
| Phase 1: Preparation and Training Phase | This phase focuses on the proactive measures required to build resilience into our IT systems and processes. It includes regular training sessions for employees, establishing and maintaining comprehensive documentation, and conducting simulation drills to test and refine our response capabilities |
| Phase 2: Activation and Notification Phase | During this phase, clear criteria and procedures are established for activating the Business Continuity Plan. This includes identifying the conditions that warrant activation, such as critical system failures or cybersecurity incidents, and implementing notification protocols to ensure prompt and efficient communication with all relevant stakeholders. |
| Phase 3: Recovery Phase | The recovery phase outlines the step-by-step procedures for restoring IT systems and business operations to their normal state. This includes damage assessment, resource allocation, data recovery, and testing to ensure that systems are functioning correctly. |
| Phase 4: Reconstitution Phase | This final phase focuses on the long-term restoration and normalization of business operations. It involves concurrent processing to validate system performance, thorough testing to ensure functionality, and effective communication to all stakeholders regarding the completion of the reconstitution process. |

# Phase 1: Preparation and Training Phase (Technology and IT Continuity Focus)

This section focuses exclusively on the preparation and training procedures related to technology and IT continuity processes. Other elements are explicitly excluded to maintain clarity and specificity.

## Roles and Responsibilities:

|  |  |
| --- | --- |
| General Guidelines | * Clearly define the roles and responsibilities of all individuals involved in IT business continuity. * Ensure that each role is linked to specific tasks and recovery procedures. * Assign roles and responsibilities to specific individuals or teams. * Ensure that all personnel understand their roles and are prepared to execute them in an emergency. * Regularly review role assignments to account for personnel changes and new hires. |

### Specific Roles and Responsibilities for Preparation and Training

|  |  |
| --- | --- |
| Role | Responsibility |
| Executive Sponsor | Provide overall guidance and support for the BCP. |
| IT Manager | Oversee the maintenance, preparation, and training activities. |
| Help Desk Lead | Coordinate help desk activities and training sessions. |
| Incident Response Coordinator | Develop training materials and lead simulation drills. |

### Process for Maintaining Business Impact Analysis (BIA), System Dependency, and Individual System Recovery Plans

|  |  |
| --- | --- |
| Regular Review and Update | **BIA Updates**: Conduct regular reviews and updates of the Business Impact Analysis to ensure it reflects current business priorities and IT infrastructure.   * Schedule BIA reviews semi-annually or when significant changes occur. * Involve key stakeholders in the review process to capture comprehensive input.   **System Dependency Mapping**: Maintain an up-to-date map of system dependencies to understand the interconnections and critical points of failure.   * Update the dependency map with each system change or new implementation. * Validate the accuracy of the dependency map through regular audits.   **Individual System Recovery Plans**: Develop and maintain detailed recovery plans for each critical IT system.   * Ensure each plan includes step-by-step recovery procedures, required resources, and estimated recovery times. * Review and update these plans annually or as systems change. |

|  |  |
| --- | --- |
| Documentation and Storage | **Centralized Repository**: All <Customer> BIA documents, system dependency maps, and individual recovery plans in the following centralized, accessible repository:   >\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Repository Requirements:   * Ensure the repository is secure and regularly backed up. * Provide access to relevant personnel based on roles and responsibilities. |

### Process for Maintaining Contact Lists and Roles/Responsibilities for Business Continuity

|  |  |
| --- | --- |
| Contact List Management | Regular Updates:   * Maintain an up-to-date contact list of all IT employees, vendors, clients, and other key stakeholders involved in business continuity. * Update contact lists quarterly or whenever there are personnel changes. * Ensure that all contact information is accurate and includes multiple methods of communication (e.g., phone, email).   Verification:   * Periodically verify contact information by conducting test notifications. * Confirm that all contacts receive notifications and can respond appropriately. |

## Training and Validation Exercises

|  |  |
| --- | --- |
| General Guidelines | Employee Training:   * Conduct regular training sessions for all IT staff to ensure they understand their roles and responsibilities in the event of an IT disruption. * Include training on specific recovery procedures, use of backup systems, and emergency communication protocols. * Offer refresher courses annually and training for new hires as part of their onboarding process.   Vendor and Partner Training:   * Involve key vendors and partners in training sessions to ensure coordinated responses during IT disruptions. * Share relevant sections of the business continuity plan and recovery procedures with vendors and partners. |

### Tabletop Exercises

Tabletop exercises are an essential part of the preparation and training phase. These exercises involve key personnel discussing their roles during an emergency and their responses to a simulated event. The exercises help to identify strengths and weaknesses in the BCP and improve the organization's preparedness.

|  |  |
| --- | --- |
| Tabletop Exercise Process | **Planning**: The Incident Response Coordinator will plan the tabletop exercise, including selecting the scenario and identifying participants.  **Execution**: During the exercise, the incident response coordinator will facilitate a discussion with participants about their responses to the scenario.  **Evaluation**: After the exercise, the Incident Response Coordinator will lead a debriefing session to evaluate the exercise and identify areas for improvement.  **Documentation**: The results and recommendations from the exercise will be documented and used to update the BCP. |

#### Tabletop Exercise Roles and Responsibilities:

| Role | Responsibility |
| --- | --- |
| Executive Sponsor | Oversee and support the tabletop exercise process. |
| IT Manager | Ensure participation from relevant IT staff and resources. |
| Help Desk Lead | Participate in the exercise and provide insights from a help desk perspective. |
| Incident Response Coordinator | Plan, facilitate, and evaluate the tabletop exercise. |

#### Tabletop Exercise Schedule and Timing Expectations:

|  |  |  |  |
| --- | --- | --- | --- |
| Activity | Responsible Role | Time Allocated | Frequency |
| Planning | Incident Response Coordinator | 4 hours | Semi-annually |
| Execution | All roles | 2 hours | Semi-annually |
| Evaluation | Incident Response Coordinator | 2 hours | Semi-annually |
| Documentation | Incident Response Coordinator | 2 hours | Semi-annually |

### Validation Exercises

|  |  |
| --- | --- |
| Backup and Restore Validation | Regular Testing:   * Conduct regular tests of backup and restore procedures to ensure data integrity and recoverability. * Schedule tests quarterly to validate the effectiveness of backup processes. * Include different types of data and systems in each test to cover all critical areas.   Validation Reports:   * Document the results of each backup and restore test. * Identify any issues or failures and take corrective actions. * Share validation reports with senior IT management and relevant stakeholders. |

|  |  |
| --- | --- |
| RTO and RPO Validation | Regular Validation:   * Regularly validate Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) to ensure they meet business requirements. * Conduct RTO and RPO validation tests semi-annually. * Simulate different types of disruptions to test the effectiveness of recovery procedures.   Performance Analysis:   * Analyze the results of RTO and RPO tests to identify gaps and areas for improvement. * Adjust recovery plans and procedures based on test results. * Ensure that all changes are documented and communicated to relevant stakeholders. |

## Schedule and Timing

Preparation and Training - Estimated Level of Effort (LOE) by Role

Initial estimates on schedule and timing include:

|  |  |  |  |
| --- | --- | --- | --- |
| Activity | Responsible Role | Time Allocated | Frequency |
| Employee Training Sessions | Help Desk Lead | 2 hours | Quarterly |
| BIA Updates | IT Manager | 4 hours | Semi-annually |
| System Dependency Mapping | Incident Response Coordinator | 3 hours | Quarterly |
| Individual System Recovery Plan Review | Help Desk Lead | 2 hours | Annually |
| Tabletop Exercises | Incident Response Coordinator | 4 hours | Semi-annually |
| Backup/ Restore Validation | IT Manager | 4[[2]](#footnote-2) hours per system validated | Semi-annually |
| RPO Validation | IT Manager | 2 hours per system validated | Semi-annually |

Preparation and Training – Yearly Calendar

|  |  |
| --- | --- |
| Month | Activity |
| January | BIA Updates |
| February | Employee Training Sessions / B/R Validation |
| March | System Dependency Mapping |
| April | RPO Validation |
| May | Tabletop Exercise |
| June | Employee Training Sessions |

|  |  |
| --- | --- |
| Month | Activity |
| July | B/R Validation |
| August | System Dependency Mapping |
| September | Employee Training Sessions |
| October | Individual System Recovery Plan Review |
| November | RPO Validation / Tabletop Exercise |
| December | System Dependency Mapping |

# Phase 2: Activation and Notification Phase

This section focuses exclusively on the activation and notification procedures related to technology and IT continuity processes. Other elements are explicitly excluded to maintain clarity and specificity.

### Specific Roles and Responsibilities for Activation and Notification

|  |  |
| --- | --- |
| Role | Responsibility |
| Executive Sponsor | Authorize the activation of the BCP |
| IT Manager | Coordinate the activation process and communication |
| Help Desk Lead | Ensure all help desk staff are informed and ready to act |
| Incident Response Coordinator | Assess the situation and communicate the activation to the relevant teams. |

## Activation Criteria

The Activation Criteria for technology and IT continuity outline the circumstances under <Client’s> Business Continuity Plan (BCP) for IT systems that should be activated when one or more of the following criteria is met:

|  |  |
| --- | --- |
| Criteria: | * *Critical System Failure*: Any key IT systems or infrastructure failure that impacts core business operations for more than 30 minutes. * *Cybersecurity Incidents*: Major breaches, ransomware attacks, or other cyber threats compromising business data or IT systems. * *Network Outages*: Significant network disruptions, including internet outages, that affect business operations. * *Data Corruption*: Instances of significant data corruption that impact the integrity and availability of critical data. * *Hardware Failures*: Critical hardware failures such as server crashes, storage device malfunctions, or significant network equipment failures. * *Software Failures*: Major software issues, including critical application crashes or failures in essential business software. |

## Notification Procedures

Effective notification procedures ensure that all relevant IT and technology stakeholders are informed promptly and clearly about the activation of the BCP. For <Acme>, these procedures may include:

* Emergency Notification System:
  + When an employee suspects a significant outage or incident is underway, they will be instructed to contact the Help Desk.
  + The Help Desk will evaluate the outage or incident to see if it rises to the level of the above criteria.
  + Upon validation, they will activate the ‘Notification Tree’ and simultaneously call the IT Manager.
* Notification Tree: The following notification process will be followed in the event of a crisis event using the contact list in the appendices of this document:

1. Initial Contact: Senior IT Management and BCP Team Leaders:

*Notification Call*: The help desk will immediately set up a triage callin Teams to coordinate activities. If Teams is unavailable, send a JitsiMeet [[3]](#footnote-3)invitation

*Method of Contact:* SMS, Teams Message, AND phone call <NOT e-mail!)

1. BCP Team

Triage Call: The help desk will set up an additional Teams call for the BCP team, which may be expanded to include additional technical resources as needed.

*Method of Contact:* SMS, Teams Message, AND phone call <NOT e-mail!)

1. Executive Management: Senior IT leadership will determine when Executive management will be notified.
2. Employees: Executive management will determine when and how employees will be notified of the event.

## Outage Assessment

The Outage Assessment process involves evaluating the extent and impact of the IT disruption on business operations. For <Acme>, the process includes:

|  |  |
| --- | --- |
| Outage Assessment Process | 1. Initial Assessment: Conduct a rapid initial assessment to determine the nature and extent of the IT outage. 2. Team Assembly: Gather the IT BCP team and relevant experts to conduct the assessment. 3. Situation Analysis: Identify the affected IT systems, applications, and processes. 4. Impact Estimation: Estimate the potential impact on business operations, data integrity, and IT services. 5. Detailed Assessment: Follow up with a more detailed assessment to gather comprehensive information. 6. Data Collection: Collect detailed data on the IT outage, including system logs, incident reports, and technical diagnostics. 7. Root Cause Analysis: Investigate the root cause of the IT outage to inform recovery efforts. 8. Resource Identification: Identify the resources needed for IT recovery, including personnel, equipment, and external support. 9. Communication of Findings: Share the findings of the IT outage assessment with senior IT management and key stakeholders. 10. Assessment Report: Prepare a detailed report outlining the findings, impacts, and recommended actions. 11. Briefings: Conduct briefings with relevant IT teams to ensure everyone understands the situation and their roles in the recovery process. 12. Continuous Monitoring: Continuously monitor the situation and update the assessment as new information becomes available. 13. Progress Updates: Regularly update stakeholders on the status of the IT outage and recovery efforts. 14. Adjustments: Make necessary adjustments to the recovery plan based on ongoing assessments and feedback. |

Schedule and Timing

Activation and Notification routine tasks - Estimated Level of Effort (LOE) by role   
Initial estimates on schedule and timing include:

|  |  |  |  |
| --- | --- | --- | --- |
| Activity | Responsible Role | Time Allocated | Frequency |
| Activation Criteria Review | IT Manager | 2 hours | Annually |
| Notification Procedure Testing | Incident Response Coordinator | 3 hours | Annually |
| Emergency Notification System Update | Help Desk Lead | 1 hour | Quarterly |
| Contact List Verification | IT Manager | 2 hours | Quarterly |

### Activation and Notification – Yearly Calendar

|  |  |
| --- | --- |
| Month | Activity |
| January | Emergency Notification System Update |
| February | Contact List Verification |
| March | -- |
| April | Emergency Notification System Update |
| May | Contact List Verification |
| June | Notification Procedure Testing |

|  |  |
| --- | --- |
| Month | Activity |
| July | Emergency Notification System Update |
| August | Contact List Verification |
| September |  |
| October | Activation Criteria Review |
| November | Emergency Notification System Update |
| December | Contact List Verification |

# Phase 3: Recovery Phase

This section focuses exclusively on the recovery procedures related to technology and IT continuity processes. Other elements are explicitly excluded to maintain clarity and specificity.

### Specific Roles and Responsibilities for the Recovery Phase:

|  |  |
| --- | --- |
| Role | Responsibility |
| Executive Sponsor | Monitor the recovery efforts and provide necessary resources. |
| IT Manager | Oversee the recovery activities and ensure timely restoration of services. |
| Help Desk Lead | Support the IT team by managing user inquiries and issues. |
| Incident Response Coordinator | Lead the recovery efforts and report progress to the Executive Sponsor. |

## Recovery Process in Sequence:

The sequence of recovery activities should be meticulously planned to ensure a swift and organized restoration of IT operations. For <Acme>, our sequence includes:

1. Safety and Security: Ensure the safety of IT personnel and secure the affected IT infrastructure.

* Conduct safety checks of IT facilities and data centers.
* Secure access to IT systems and areas to prevent unauthorized access.

### Prioritize IT Recovery Tasks.

* Resource Allocation: Leverage the information gathered during the Outage Assessment process and assign IT resources (personnel, equipment, and materials) based on the priorities established in that phase
* Mobilize internal IT teams and external vendors as needed.

1. Infrastructure Restoration: Begin with restoring essential IT infrastructure and utilities.

* Restore power, cooling systems, and telecommunications to IT facilities.
* Ensure backup generators and other emergency systems are operational for IT infrastructure.

1. Data Recovery: Focus on recovering critical data and IT systems.

* Restore data from backups and ensure data integrity.
* Reboot and test critical IT applications and systems.

1. IT Operations Restoration: Restore key IT operations in a phased approach, starting with the most critical systems.

* Resume core IT processes and services.
* Gradually reinstate less critical IT functions.

1. Testing and Validation: Test restored IT systems and processes to ensure they function correctly.

* Conduct functional and performance testing on IT systems.
* Validate the integrity of recovered data and applications.

1. Communication: Keep all IT stakeholders informed throughout the recovery process.

* Provide regular updates to IT staff, vendors, and relevant business units.
* Use multiple communication channels to ensure information reaches all relevant IT stakeholders.

1. Continuous Monitoring: Monitor the recovery process and adjust as needed.

* Track progress against the IT recovery plan.
* Identify and address any issues or obstacles that arise during IT recovery.

Schedule and Timing

### Recovery Phase Tasks - Estimated Level of Effort (LOE) by Role

Initial estimates on schedule and timing include:

|  |  |  |  |
| --- | --- | --- | --- |
| Activity | Responsible Role | Time Allocated | Frequency |
| Damage Assessment | IT Manager | 4 hours | As needed |
| Resource Allocation | Executive Sponsor | 2 hours | As needed |
| Systems and Data Recovery | IT Manager | TBD – based on the level of outage | As needed |
| IT Operations Restoration | IT Manager | 8 hours | As needed |
| Recovery Progress Updates | Incident Response Coordinator | 1 hour | Daily during recovery |

# Phase 4: Reconstitution Phase

This section focuses on the reconstitution procedures related to technology and IT continuity processes. Other elements are explicitly excluded to maintain clarity and specificity.

## Concurrent Processing

During the reconstitution phase, concurrent processing involves operating both the restored IT systems and the backup systems simultaneously to ensure a smooth transition back to normal operations.

Parallel Operations:

* Run the restored primary IT systems alongside the backup systems to validate their performance and stability.
* Monitor both systems closely for discrepancies.
* Ensure that data synchronization is maintained between the primary and backup systems.
* Performance Monitoring: Continuously monitor the performance of the primary systems.
* Track system loads, response times, and error rates.
* Identify and resolve any performance issues promptly.

Gradual Transition:

* Gradually shift processing loads from backup systems to primary systems.
* Implement a phased approach to avoid overloading any single system.
* Validate each step before proceeding to the next phase.

## Testing

Testing is crucial to ensure all IT systems and applications are fully functional and meet performance standards.

Functional Testing:

* Perform comprehensive functional tests on all restored IT systems.
* Verify that each application and service operates as expected.
* Conduct user acceptance testing (UAT) with key stakeholders.

### Integration Testing:

* Test the integration points between various IT systems and applications.
* Ensure seamless communication and data exchange between systems.

### Load Testing:

* Simulate high-usage scenarios to evaluate system performance under stress.
* Identify potential bottlenecks and address them before full-scale operations resume.

### Security Testing:

* Conduct thorough security assessments to ensure the restored systems are secure.
* Perform vulnerability scans and penetration tests.
* Ensure that all security controls and measures are in place and effective.

## Notifications

Effective notifications keep all relevant IT stakeholders informed about the progress and completion of the reconstitution phase.

Stakeholder Updates:

* Provide regular updates to all IT stakeholders, including employees, vendors, and clients.
* Use multiple communication channels (e.g., email, intranet, secure messaging) to ensure information reaches everyone.

Completion Announcement:

* Notify stakeholders when the reconstitution phase is complete.
* Clearly communicate the return to normal operations.
* Provide details on any changes or improvements made during the reconstitution.

### Feedback Request:

* Solicit feedback from stakeholders on the reconstitution process.
* Use feedback to identify areas for improvement and enhance future continuity plans.

## Cleanup

Cleanup activities ensure that all temporary measures and resources used during the recovery are appropriately managed and documented.

### Temporary Infrastructure:

* Decommission any temporary IT infrastructure set up during the recovery phase.
* Safely remove temporary servers, networking equipment, and workstations.
* Ensure proper disposal or storage of temporary resources.

### Data Cleanup:

* Ensure that all temporary data used during recovery is securely deleted or archived as needed.
* Verify data integrity and consistency across all systems.

### Resource Reallocation:

* Reallocate IT resources (personnel, equipment) to their regular roles and responsibilities.
* Ensure all IT staff are informed of their post-recovery duties.

## Documentation

Comprehensive documentation of the reconstitution process and IT systems is essential for future reference and continuity planning.

### Process Documentation:

* Document all steps taken during the reconstitution phase.
* Include detailed procedures, timelines, and personnel involved.

### System Documentation:

* Update documentation for all IT systems and applications.
* Include system configurations, network diagrams, and data flows.

### Lessons Learned:

* Compile a lessons learned report to identify successes and areas for improvement.
* Use this information to enhance future IT continuity and recovery plans.

### Policy Updates:

* Review and update IT policies and procedures based on the reconstitution experience.
* Ensure all changes are communicated to relevant stakeholders and incorporated into training programs.

### Final Summary Report:

* Create a final summary report from the incident for the executive team
* Recap the essential timeline, root cause, recovery effort, and current state
* Identify any requirements/recommendations for notifying end customers, contract management, and/or law enforcement.
* Conclude with lessons learned and identify changes in the process that will integrate those lessons learned into the revised BC process.

# Appendix A – Contact List

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Role | Name | Title | Email | Cell | Time Zone |
| Executive Sponsor | Daniel Radcliff | CIO | [dradcliff@company.com](mailto:dradcliff@company.com) | 555.121.1234 | EST |
| IT Manager |  |  |  |  |  |
| Help Desk Lead |  |  |  |  |  |
| Incident Response Coordinator |  |  |  |  |  |
| BCP Team Leader |  |  |  |  |  |
| Incident Response Team: IT Lead |  |  |  |  |  |
| Incident Response Team: Cybersecurity Lead |  |  |  |  |  |
| Incident Response Team: Network Lead |  |  |  |  |  |
| Incident Response Team: Application Lead |  |  |  |  |  |
| Incident Response Team: Business Lead |  |  |  |  |  |

# Appendix B – Risks Considered

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Environmental | | Supply Chain | Economic | Labor | Facilities | Technology | Legal |
| Major power outage | | Supplier failure | Market downturn | Workforce strikes/ unionization | Fire | Cyberattacks | Regulatory compliance |
| Hurricane | | Transportation delays | Currency fluctuations | Talent shortages | Structural damage | Data breaches | Intellectual property disputes |
| Earthquake | | Raw material shortages | Inflation | High turnover | Theft or vandalism | System outages | Contract breaches |
| Flood | | Import/export restrictions | Interest rate changes | Health pandemics | Hazardous material spill | Software failures | Lawsuits |
| Tornado | | Quality issues | Economic sanctions | Regulatory changes | HVAC failure | Hardware failures | Labor law violations |
| Wildfire | | Political instability | Trade policy changes | Workplace accidents | Water damage | Emerging technology risks | Environmental regulations |
|  | |  |  |  |  | Insider Sabotage | Ransomware |
|  | |  |  |  |  | Admin Error |  |
|  | |  |  |  |  | Backup System Failure |  |
|  | |  |  |  |  | Ransomware |  |
|  | |  |  |  |  | Cloud Service Outage |  |
| KEY: | Risks in RED are the focus of the Business Continuity Program | | | | | | |

# Appendix C – Major Business Process to BU Map

| Major Business Function | BP Reference # | Business Process | Description | Owner | Centralized (Yes/No) | Business Unit | Criticality (High/ Med/Low) |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Sales | Sales.SO.1 | Sales Operations | Managing sales pipeline and customer acquisition | John Doe | Yes | Sales Dept | High |
| Marketing | MKT.MP.01 | Market Planning | Planning and executing marketing strategies | Sarah Davis | Yes | Marketing Dept | High |
| Marketing | MKT.PR.02 | Public Relations | Managing public relations and media communications | Mike Green | No | Marketing Dept | Medium |
| Manufacturing | MFG.PM.01 | Production Management | Overseeing production processes and ensuring quality control | Emily White | Yes | Manufacturing | High |
| Manufacturing | MFG.IN.02 | Inventory Management | Managing inventory levels and materials procurement | Tom Black | No | Manufacturing | Medium |
| Service | SVC.MA.01 | Maintenance | Performing regular maintenance on products and equipment | Laura Brown | No | Service Dept | Medium |
| Service | SVC.FS.02 | Field Services | Providing on-site services and support to clients | Kevin Blue | No | Service Dept | Medium |
| Customer Support | CS.SD.01 | Support Desk | Handling customer inquiries and support tickets | Jane Smith | No | Support Dept | Medium |
| Customer Support | CS.TC.02 | Technical Support | Providing technical assistance and troubleshooting | Robert King | Yes | Support Dept | High |
| Human Resources | HR.BM.01 | Benefits Management | Managing and administrating benefits for employees | Mark Johnson | Yes | HR | High |
| Human Resources | HR.TM.02 | Talent Management | Recruitment, training, and employee development | Susan Lee | Yes | HR | High |
| Information Technology | IT.HD.01 | Help Desk | Managing inbound calls, email, and chat requests for support | Alice Brown | No | IT | High |
| Information Technology | IT.IM.02 | Infrastructure Management | Managing and maintaining IT infrastructure | Steven Clark | Yes | IT | High |
| Information Technology | IT.SO.03 | Security Operations | Monitor and respond to cyber events | Tom Jones | Yes | IT | High |
| Information Technology | IT.MM.04 | Device Management | Procure, retire computer and mobile equipment | Stephen Jenkins | Yes | IT | Medium |
| Accounting/Finance | AF.AR.01 | Accounts Receivable | Managing incoming payments and customer accounts | Mary Adams | Yes | Finance Dept | High |
| Accounting/Finance | AF.AP.02 | Accounts Payable | Managing outgoing payments and vendor accounts | David White | Yes | Finance Dept | Medium |
| Accounting/Finance | AF.PR.01 | Procurement | Ordering and managing supply chain logistics | Sarah Bess | Yes | Finance Dept | High |
| Legal | Legal.CL.01 | Contract Law | Drafting, reviewing, and managing contracts | Karen Wright | Yes | Legal Dept | High |
| Legal | Legal.CR.02 | Compliance and Regulations | Ensuring company compliance with legal and regulatory requirements | John Smith | Yes | Legal Dept | High |
| Operations Management | OM.SP.01 | Strategic Planning | Developing and implementing long-term business strategies | Lisa Green | Yes | Operations Dept | High |
| Operations Management | OM.PM.02 | Project Management | Managing projects and ensuring timely delivery | Greg Brown | No | Operations Dept | Medium |
| ‘Centralized' Designation Requirement | Does the business process utilize 'core company' personnel, essential processes, and technologies? | | | | | | |

# Appendix D – Business Process to Technology Map

| Business Process | Potential Impact if Unavailable | Description | Component Workflow | Dependent Technology | Technology ID | Max Tolerable Downtime (MTD) | Recovery Point Objective (RPO) |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Sales Operations | Loss of potential sales and revenue | Managing sales pipeline and customer acquisition | Lead Generation → Lead Nurturing → Closing Sales | Salesforce | SFDC | 24 hours | 1 hour |
| Market Planning | Delay in marketing campaigns and loss of market opportunities | Planning and executing marketing strategies | Market Research → Campaign Design → Campaign Execution | Marketing Automation Software | MAS.01 | 48 hours | 2 hours |
| Public Relations | Damage to company reputation and public image | Managing public relations and media communications | Press Release Creation → Distribution → Media Follow-up | PR Management Software | PRM.01 | 72 hours | 4 hours |
| Email Marketing | Loss of communication with prospects and customers | Email marketing initiatives, including newsletters, B2B sales outreach, etc. | Lead Management -> Marketing Collaboration -> Email Automation | Email Marketing Platform | EMP.01 | 72 hours | 8 hours |
| Social Media Marketing - LinkedIn | Reduced brand visibility and engagement | Social media marketing, content marketing, blogging, and public perception management on LinkedIn | Lead Management -> Marketing Collaboration -> LinkedIn | LinkedIn | LI | 72 hours | 8 hours |
| Social Media Marketing - Facebook | Reduced brand visibility and engagement | Social media marketing, content marketing, blogging, and public perception management on LinkedIn | Lead Management -> Marketing Collaboration -> Facebook | Facebook | FB | 72 hours | 8 hours |
| Production Management | Delays in production and potential quality issues | Overseeing production processes and ensuring quality control | Production Scheduling → Manufacturing → Quality Inspection | NetSuite | ERP.NS.01 | 12 hours | 1 hour |
| Inventory Management | Stockouts or overstock issues impacting production and sales | Managing inventory levels and materials procurement | Order Placement → Inventory Monitoring → Reordering | Inventory Management Software | IMS.01 | 48 hours | 4 hours |
| Maintenance | Increased equipment downtime and repair costs | Performing regular maintenance on products and equipment | Maintenance Scheduling → Maintenance Execution → Reporting | Maintenance Management System | MMS.01 | 72 hours | 8 hours |
| Field Services | Delays in service delivery and customer dissatisfaction | Providing on-site services and support to clients | Service Request → Dispatch → On-Site Service | Field Service Management Software | FSM.01 | 24 hours | 4 hours |
| Support Desk | Increased customer complaints and unresolved issues | Handling customer inquiries and support tickets | Ticket Creation → Issue Diagnosis → Resolution | Support Ticketing System | STS.01 | 4 hours | 30 minutes |
| Technical Support | Prolonged system downtime and user frustration | Providing technical assistance and troubleshooting | Issue Identification → Troubleshooting → Solution Deployment | Remote Support Tools | RS.Kasaya.01 | 8 hours | 1 hour |
| Benefits Management | Employee dissatisfaction and potential compliance issues | Managing and administrating benefits for employees | Benefit Enrollment → Claims Processing → Benefit Auditing | HR Management Software | ADP | 48 hours | 4 hours |
| Talent Management | Delays in hiring and onboarding new employees | Recruitment, training, and employee development | Job Posting → Candidate Screening → Onboarding | Applicant Tracking System | ATS.01 | 72 hours | 8 hours |
| Help Desk | Reduced IT support efficiency and increased downtime | Managing inbound calls, email, and chat requests for support | Ticket Logging → Issue Assignment → Resolution | IT Service Management Software | ITSM.01 | 4 hours | 30 minutes |
| Infrastructure Management | Prolonged IT infrastructure issues affecting business operations | Managing and maintaining IT infrastructure | Infrastructure Monitoring → Maintenance → Upgrades | Network Management Tools | NMS.01 | 12 hours | 1 hour |
| Accounts Receivable | Delays in cash flow and financial reconciliation | Managing incoming payments and customer accounts | Invoice Generation → Payment Processing → Reconciliation | NetSuite | ERP.NS.01 | 24 hours | 2 hours |
| Accounts Payable | Payment delays and potential vendor relationship issues | Managing outgoing payments and vendor accounts | Invoice Receipt → Payment Authorization → Payment Processing | NetSuite | ERP.NS.01 | 48 hours | 4 hours |
| Contract Law | Delays in contract processing and potential legal risks | Drafting, reviewing, and managing contracts | Contract Drafting → Review → Approval | Salesforce | SFDC | 72 hours | 8 hours |
| Compliance and Regulations | Regulatory penalties and increased risk exposure | Ensuring company compliance with legal and regulatory requirements | Compliance Audit → Reporting → Remediation | Compliance Management Software | GRC.01 | 48 hours | 4 hours |
| Strategic Planning | Delays in strategic decision-making and goal achievement | Developing and implementing long-term business strategies | SWOT Analysis → Goal Setting → Strategy Implementation | PowerBI | BI.PowerBI.01 | 72 hours | 8 hours |
| Project Management | Project delays and missed deadlines | Managing projects and ensuring timely delivery | Project Initiation → Planning → Execution → Closure | Microsoft Project Server | MSPS.01 | 24 hours | 2 hours |

# Appendix E – Technology RTO

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Dependent Technology | Technology ID | Max Tolerable Downtime (MTD) | Recovery Point Objective (RPO) | System Components (name) | Dependent Subcomponents (name) | RTO |
| Salesforce | SFDC | 24 hours | 1 hour | SFDC Cloud | Internet Access | 24 hours |
| Marketing Automation Software | MAS.01 | 48 hours | 2 hours | MASWeb01 | DCSwitch01 | 48 hours |
|  |  |  |  | MASWeb01 | MainFW01 | 48 hours |
|  |  |  |  | CUSTSQL01 | DCSAN01 | 48 hours |
|  |  |  |  | CUSTSQL01 | DCSAN-Switch01 | 48 hours |
|  |  |  |  | CUSTSQL01 | DCFW01 | 4 hours |
|  |  |  |  | CUSTSQL01 | DCSwitch01 | 4 hours |
|  |  |  |  | MASApp01 | MSLS01 (license server) | 4 hours |
|  |  |  |  | MASApp01 | DCFW01 | 4 hours |
|  |  |  |  | MASApp01 | DCSwitch01 | 4 hours |
| Support Ticketing System | STS.01 | 4 hours | 30 minutes | CUSTSQL01 | DCSAN01 | 4 hours |
|  |  |  |  | CUSTSQL01 | DCSAN-Switch01 | 4 hours |
|  |  |  |  | CUSTSQL01 | DCFW01 | 4 hours |
|  |  |  |  | CUSTSQL01 | DCSwitch01 | 4 hours |
|  |  |  |  | STSApp01 | MSLS01 (license server) | 4 hours |
|  |  |  |  | STSApp01 | DCSwitch01 | 4 hours |
|  |  |  |  | STSApp01 | DCFW01 | 4 hours |

# Appendix F – Example Tabletop Exercise Outline

## Purpose

This tabletop exercise evaluates the organization's preparedness and ability to effectively execute the recovery and reconstitution phases of the Business Continuity Plan (BCP). It will involve key stakeholders identified in the plan, benchmark participants' ability to follow essential processes, and conclude with a measurable grade for the team's fidelity to the process.

## Scenario

A significant cyber-attack has compromised the organization's primary IT systems, leading to a critical system failure. The exercise will simulate the steps necessary for recovery and reconstitution to ensure business continuity.

## Participants

Utilize the ‘Contact Information’ section of this document to establish contact with these stakeholders:

|  |
| --- |
| Role |
| Executive Sponsor |
| IT Manager |
| Help Desk Lead |
| Incident Response Coordinator |
| BCP Team Leader |

## Exercise Phases

### 1. Initial Briefing

**Duration**: 30 minutes

* + Welcome and introduction by the Executive Sponsor
  + Overview of the scenario and objectives by the Incident Response Coordinator
  + Distribution of materials (scenario details, roles and responsibilities, process flowcharts)

### 2. Scenario Presentation

**Duration**: 15 minutes

* Incident Response Coordinator presents the details of the cyber-attack scenario
* Outline the current state of IT systems and the impact on business operations

### 3. Recovery Phase Simulation

**Duration**: 2 Hours

Activities:

1. Damage Assessment

* The IT Manager leads the team in conducting a thorough assessment of the damage to IT systems.
* Document findings and prioritize recovery tasks.

2. Resource Allocation

* Executive Sponsor ensures necessary resources are available.
* IT Manager coordinates the mobilization of internal IT teams and external vendors.

3. Data Recovery

* Incident Response Coordinator leads the data recovery efforts.
* Ensure data integrity and restore critical IT applications.

4. IT Operations Restoration

* IT Manager oversees the phased restoration of key IT operations.
* Help Desk Lead supports user inquiries and issues.

### 4. Reconstitution Phase Simulation

**Duration**: 2 hours

Activities:

1. Concurrent Processing Monitoring

* IT Manager monitors the performance of restored primary IT systems.

2. Functional Testing

* Incident Response Coordinator conducts comprehensive functional tests on restored systems.

3. Integration and Load Testing

* IT Manager and Incident Response Coordinator perform integration and load testing.

4. Security Testing

* Incident Response Coordinator conducts security assessments to ensure system security.

5. Final Testing and Validation

* Incident Response Coordinator validates the reconstitution process and documents lessons learned.

### Debriefing and Evaluation

**Duration**: 1 hour

* Incident Response Coordinator leads a debriefing session
  + Discuss what went well and what could be improved
  + Gather feedback from participants
* The Executive Sponsor reviews the overall performance
* Participants complete evaluation forms

### Evaluation Criteria

The following criteria will be used to measure the team's fidelity to the process:

|  |  |
| --- | --- |
| Criteria | Score |
| Damage Assessment Accuracy |  |
| Resource Allocation Efficiency |  |
| Data Recovery Effectiveness |  |
| IT Operations Restoration Timeliness |  |
| Concurrent Processing Monitoring |  |
| Functional Testing Thoroughness |  |
| Integration and Load Testing Accuracy |  |
| Security Testing Completeness |  |
| Final Testing and Validation |  |
| Communication and Coordination |  |

Scoring:

1: Poor

2: Fair

3: Good

4: Very Good

5: Excellent

### Final Grade

The final grade will be an average of the scores for each criterion. This will provide a measurable assessment of the team's performance during the tabletop exercise.

### Follow-up Actions

* Update the Business Continuity Plan based on findings and feedback from the exercise.
* Schedule additional training or drills if necessary.
* Conduct a follow-up tabletop exercise to address identified weaknesses.

1. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf [↑](#footnote-ref-1)
2. Number of hours per system restored should be relatively close to the RTO of the system in question. In addition to validating RTO, the actual system contents should be programmatically verified as ‘viable’ for production operations. Having a ‘green light’ report of a successful restore isn't enough! [↑](#footnote-ref-2)
3. https://meet.jit.si/ [↑](#footnote-ref-3)