Business Continuity Plan

Liam Dodd

April 8, 2024

Introduction

Business continuity planning (BCP) is a critical component of building organizational resilience. BCP involves creating strategies and plans to ensure that key business functions can continue operating in the event of a disruption. This allows organizations to respond and recover more quickly from incidents like natural disasters, cyber attacks, supply chain issues, or other crises. Effective business continuity planning is significant for organizational resilience for several reasons:

- It minimizes downtime and service disruptions by implementing resilience strategies like redundancy, backup systems, and alternative work arrangements. This maintains continuity of critical operations during and after a disruption.
- It provides a roadmap for incident response and recovery. Detailed response and recovery plans guide actions to stabilize the situation, restore operations, and return to normal. This organized approach prevents ad hoc reactions that may be less effective.
- It builds organizational adaptability and the capability to manage unforeseen threats. Scenario analysis during planning strengthens abilities to handle a range of potential incidents.
- It reassures stakeholders like customers, regulators, investors, and employees that the organization can withstand and recover from disruptions. This maintains trust and confidence in the organization.

In summary, business continuity planning enables organizational resilience by preparing an organization to quickly adapt and rebound when faced with disruptive events. It provides a tested framework for minimizing impacts and restoring critical operations needed for survival and competitiveness. This capability is increasingly important in today's complex and turbulent business environment.

Risk Assessment and Business Impact Analysis

VISION Health's core assets include sensitive patient data, intellectual property, financial data, and physical infrastructure. A disruption to any of these assets could significantly impact operations and finances.

Key external dependencies are relationships with healthcare clients and vendors. Issues with client security or vendor negligence could propagate risk back to VISION.

Top risks requiring mitigation are around data privacy, security architecture, operations, communications, and business continuity.

Key Assets

- Patient data
  - Medical records, imaging, PII
  - Highly sensitive information

- Intellectual property
  - Algorithms, models, code
  - Competitive advantage
- Physical infrastructure
  - Servers, computers, medical devices
- Financial data
  - Billing, payments, accounting

Top Business Disruptions

- Data breach
  - Leak of patient data
  - Huge legal, financial, and reputational impact
- Service outage
  - DDoS, ransomware, or insider attack
  - Disrupts operations and revenue
- Intellectual property theft
  - Competitors steal IP
  - Loss of competitive advantage
- Non-compliance fines
  - Violations of regulations
  - Large financial impact
- Vendor negligence
  - Vendor actions lead to breach
  - Damages client relationships

Business Continuity Strategy

The overarching strategy to maintain critical operations during disruptions is to:

- Identify critical business functions and processes that are essential for ongoing operations. These may include revenue-generating activities, customer-facing services, compliance obligations, etc.
- Conduct a business impact analysis to understand the impacts of potential disruptions to these critical functions, including financial, legal, reputational, and other consequences.
- Develop continuity and recovery plans that outline responses to potential disruptions. This includes planning for backup systems, alternative locations, staffing contingencies, and other resilience measures tailored to the critical needs identified.
- Maintain ongoing readiness through testing, training, monitoring, and updating plans. Test continuity plans regularly, provide training to ensure staff understand their roles, monitor threats and risk landscape for changes, and update plans accordingly.

- Leverage redundancies in systems, data, facilities, and networks to avoid single points of failure. Build in backup capabilities, alternate sites, and diversity to mitigate localized disruptions.
- Coordinate with partners, suppliers, and vendors to align on continuity strategies. Understand their capabilities and ensure contracts include appropriate provisions.
- Incorporate lessons learned from actual disruptions into future continuity planning. Conduct thorough post-disruption reviews.

The goal is to implement cost-effective measures that reduce vulnerability to disruptions and allow rapid restoration of critical operations as needed. This provides organizational resilience when faced with potential threats.

Backup and Recovery Plan

Backup Strategy

- Database backups will be performed daily. Backups will be retained for 2 weeks.
- Application code will be stored in a version control system (Git) so all code revisions will be available. The Git repository will be backed up weekly.
- Filesystem backups of user files and other application data will be performed weekly. Backups will be retained for 4 weeks.

Recovery Strategy

- In case of database failure/data loss, the database will be restored from the most recent clean backup. Transactions since the last backup may not be recoverable.
- To recover application code, the codebase can be restored from the most recent Git repository backup or cloned from the hosted Git repository.
- To recover lost files or application data, the latest weekly backup will be used to restore the filesystem.

Monitoring

- Backup jobs will be monitored for success/failure. Backup failures will trigger alerts to the dev ops team.
- Server health monitoring will be implemented to detect system failures and trigger alerts.

Regular Testing

- Backup recovery testing will be performed quarterly by restoring backups to a test environment and verifying integrity.
- Failover testing will be performed bi-annually to ensure the recovery procedures are effective.

Communication Plan

Notification System

- An email distribution list will be created that includes all key stakeholders (list names and roles here). This list will be used for mass communication.
- A group chat will be established on a platform like Slack or Microsoft Teams to allow for real-time updates. All stakeholders will be added to this group.

Status Updates

- If a disruption occurs, the Project Manager will immediately notify stakeholders via the email distribution list and group chat.
- Regular status update emails will be sent every 4 hours by the Project Manager until the disruption is resolved. Updates will include:
  - Current status of the disruption
  - Impact to schedule, budget, etc
  - Action being taken to resolve the disruption
  - Estimated time to resolution

Escalation

- If the disruption lasts more than 8 hours, the Project Manager will schedule a conference call/video meeting to discuss the issue in more detail and answer any questions.
- If the disruption lasts more than 24 hours, the Project Manager will escalate to {senior management role} to become directly involved.

Post-Disruption Review

- Once normal operations resume, the Project Manager will schedule a meeting to review the disruption, analyze the response, and identify improvements for future communication plans. Feedback will be solicited from stakeholders.

This plan will ensure timely and transparent communication to stakeholders during any disruptions to the project. The project team is committed to keeping stakeholders informed of status and progress.

Requirements

- Identify critical business functions and processes that must be continued in the event of a disruption
- Determine RTO and RPO for each critical function and process
- Document detailed procedures for responding to various types of disruptions (e.g. power outage, cyber attack, natural disaster)
- Define roles and responsibilities for executing the plan

- Establish clear invocation criteria and procedures for activating the plan
- Implement redundant infrastructure and backups to support continued operations
- Validate the plan through testing exercises and drills
- Establish ongoing maintenance procedures to keep the plan updated
- Provide training to ensure personnel understand their responsibilities
- Integrate the plan with other policies like disaster recovery, crisis communications etc.
- Obtain senior management approval and support for the plan

Recommendations

- Conduct a risk assessment and business impact analysis to identify critical business functions and processes. Assess potential disruptions and impacts.
- Develop resilience strategies such as redundancy, backup systems, and alternative arrangements to maintain continuity of critical operations.
- Create detailed response and recovery plans outlining actions to take during disruptions. Maintain and test these plans.
- Implement backup systems and procedures for data, code, and other assets. Test backup recovery regularly.
- Incorporate lessons learned from real disruptions into future continuity planning.
- Coordinate with partners and vendors on aligned continuity strategies.
- Provide training and ensure staff understand their roles in continuity plans.

Conclusion

An effective business continuity plan is essential for organizational resilience. This plan has outlined strategies and requirements for minimizing disruptions and restoring critical operations quickly. If implemented successfully, it will reduce downtime, support stakeholder confidence, and strengthen the organization's capability to manage unforeseen threats. The project team is committed to developing a robust continuity plan that enables organizational adaptability and rapid recovery from potential disruptions.