



The Need for Business Continuity

In order for an organization to be in business, it must do business. When an emergency or disruption to business occurs, a company can lose much more than just its reputation. Natural disasters, terrorism, technological failure, or human error carry with them inherent dangers. No matter how large or how small, every organization must cope with potential loss. Business continuity planning provides the means to ensure continued operations and prevent loss of or damage to business activity and assets. Based on the business impact analysis (BIA) and risk assessment, the organization then plans, writes, tests, and updates a business continuity plan. The plan, in turn, defines the strategies and actions the organization will take to preserve its continuity.

One thing to keep in mind is that terminology varies widely among standards. Many refer to business continuity planning as contingency planning or disaster recovery. Others, like CobiT (Control Objectives for Information and related Technology), focus more on IT continuity planning. IT (systems) continuity is itself a subset of business continuity, and represents threats to technology rather than to the company as a whole. The business continuity process encompasses all such plans. Let's look at the need for Business Continuity Planning by industry, business function or government standard.

Public Companies

The AICPA Suitable Trust Services Criteria provides assurance for system availability and proper processing. It requires the need for backup and restoration through the comprehensive implementation and testing of a business continuity plan. The Turnbull guidance mentions communication of business continuity issues, indicating but not directly calling for business continuity.

NASD/NYSE

Rules 3510 and 446, of the NASD and NYSE respectively, specifically address the need for business continuity planning. The rules require the development, maintenance, review, and update of business continuity and contingency plans.



Banking/Finance

All financial standards recognize the need for business continuity. Gramm-Leach-Bliley, FFIEC (Federal Financial Institutions Examination Council), and the Sound Practices of Operational Risk call for banks and financial institutions to develop business continuity plans.

Sound Practices of Operational Risk

Because a severe event may occur beyond a bank's control, preventing it from fulfilling some of its business obligations, it is important for a bank to have a disaster recovery plan. To create a good one, the bank needs to take into account all the different types of plausible scenarios to which the bank may be vulnerable. Then the bank should identify critical business processes, including those where there is dependence on external vendors/other third parties for which rapid resumption of service would be most essential. Periodically, the bank should review their disaster recovery and business continuity plans to make sure they're consistent with the bank's current operations and business strategies. The plans should also be tested frequently to ensure that they are executable and effective.

FFIEC Information Security

Business continuity plans should be created and regularly reviewed as an integral part of the security process. Any risk assessments conducted should consider the changing risks that appear in business continuity scenarios so an appropriate security approach can be established. Strategies should consider what risks affect the organization in the event that continuity plans need to be implemented. Staff should be appropriately trained for their security roles, and all security plans surrounding the implementation of a business continuity plan should be tested alongside the business continuity plan.

FFIEC Business Continuity Planning

This booklet defines business continuity planning as "the process whereby financial institutions ensure the maintenance or recovery of operations, including services to customers, when confronted with adverse events such as natural disasters, technological failures, human error, or terrorism. If you change business processes, you must change the BCP (business continuity plan).

The plan should be reviewed regularly against benchmarks for an effective plan. Particular care should be taken to ensure that the BCP takes into account the potential for wide-area disasters that impact an entire region.

FFIEC Operations

To ensure uninterrupted product and service delivery, operations management should develop a business continuity plan (BCP). At a basic level, the plan should allow you to implement a system robust enough to deal with ordinary interruptions to operations and to facilitate prompt restoration without escalating to more drastic and costly disaster recovery procedures.



Healthcare

HIPAA requires the establishment and implementation of a contingency plan for any organization storing electronically protected health information.

HIPAA

A compliant continuity plan includes an applications and data criticality analysis, a data backup plan, a disaster recovery plan, an emergency mode operation plan, and testing and revision procedures. The plan is scalable depending on what organizations of different sizes need.

Consumer Facing

The Visa CISP calls for organizations to create an "incident response plan" in the event of a security breach.

Visa CISP

The disaster recovery plan should include a crisis-management team to handle important decisions and training for staff so they know their emergency roles. The plan should be tested at least annually.

Government

Both NIST 800-53 and the National Strategy to Secure Cyberspace call for contingency planning in government agencies. Both standards require the development and implementation of contingency plans.

NIST 800-53

The business continuity plan should be developed, distributed, and regularly updated by the organization. The plan should be formally documented and address purpose, scope, roles, responsibilities, and compliance. Any important procedures necessary to implement the business continuity plan should also be documented.

To ensure business continuity plan success, it should be integrated with other important plans such as the Disaster Recovery Plan, Continuity of Operations Plan, Incident Response Plan, and Business Recovery Plan.

Staff should be trained on how to do their part in an emergency situation. Refresher training should also be provided so they stay on top of their work.



NIST 800-53 *continued*

A completed continuity plan should be tested to ascertain whether it functions at all, and if it does function, whether it functions effectively. The plan should be regularly updated to reflect the current state of the business.

Some aspects of a continuity plan you may wish to consider including:

- A storage site that is geographically separate from the primary storage site, but close enough to facilitate timely recovery.
- An alternate processing site that is geographically separate from the primary processing site, fully configured to handle primary processing, has priority of service provisions, and has a way to deal with accessibility problems in the event of an area-wide disruption.
- Alternate telecommunications services with agreements containing priority of service provisions in accordance with the organization's availability requirements, setups that do not share a single point of failure with primary telecommunications services, service providers that are sufficiently separate from the primary service providers, and overall, service providers with adequate continuity plans of their own.

Information system backup with backup information being tested. The backup information should be used in the restoration of information system functions as part of contingency plan testing, along with stores of backup copies of the operation system and other critical system information.

National Cyberspace Strategy

America needs a national cyber disaster recovery plan involving public institutions, private institutions, and cyber centers. These centers will perform analysis, monitor use, enable information exchange, and facilitate restoration efforts.

Records Management

Records management standards do not directly call for business continuity planning.



General Standards

CobiT, NIST, COSO, the ISF Standard, OECD, and ISO 17799 all call for business continuity planning. While CobiT refers to an overall business continuity plan, it primarily addresses IT continuity planning.

CobiT Control Objectives

CobiT suggests seven areas for ensuring continuous service: IT Continuity Framework, IT Continuity Plan Strategy and Philosophy, IT Continuity Plan Contents, Minimizing IT Continuity Requirements, Maintaining the IT Continuity Plan, and Testing the IT Continuity Plan.

The IT Continuity framework is where the roles, responsibilities, and chosen approach to business continuity are laid out, along with the rules and structures for documenting the continuity plan. The IT Continuity Plan strategy and philosophy involves management ensuring that the plan is in line with the overall business continuity plan for the sake of consistency.

The actual IT continuity plan itself should contain the following:

- Guidelines on how to use the continuity plan.
- Response procedures meant to bring the business back to the state it was in before the incident or disaster.
- Recovery procedures meant to bring the business back to the state it was in before the incident or disaster.
- Procedures to safeguard and reconstruct the home site.
- Coordination procedures with public authorities.
- Communication procedures with stakeholders, employees, key customers, critical suppliers, stockholders, and management.
- Critical information on continuity teams, affected staff, customers, suppliers, public authorities, and media.

General Standards

NIST 800-14

The organization's business plan should identify functions and set priorities for them, so that in the event of disaster, the organization can avoid performing least important functions; the prioritizations should be approved by senior management.

OECD (Organization for Economic Co-operation and Development) Risk Checklist Policies, procedures, and standards that govern security requirements should address:

- Due diligence requirements
- Security service level and operational readiness requirements
- The general security scope and timing of third-party assurance reviews (e.g., SAS70 Level II, SysTrust, WebTrust certifications).
- Existence and adequacy of insurance to protect against financial losses due to third-party negligence and/or unauthorized access to service provider systems.
- Privacy policy
- Disaster recovery and business continuity plan
- Process of change management

ISO 17799

According to this international standard, there should be a managed process in place for developing a business continuity plan that brings together a variety of key elements:

- Understanding risks the organization faces in terms of their likelihood and impact, including an identification and prioritization of critical business processes.
- Understanding the impact that interruptions are likely to have on the business.
- Considering the purchase of suitable insurance, which may form part of the business continuity process.
- Formulating and documenting a business continuity strategy consistent with the agreed business objectives and priorities.
- Formulating and documenting business continuity plans in line with the agreed strategy.
- Regular testing and updating of the plans and processes put in place.
- Ensuring that the management of business continuity is incorporated in the organization's processes and structure.