

Business Continuity Management Standards – A Side-by-Side Comparison

By Brian Zawada (CBCP) & Jared Schwartz (CBCP), Protiviti

Whether your organization has begun a grassroots initiative to develop a business continuity plan or has started to wrap-up the initial implementation of a continuity management process, the need to continually revisit and improve the Business Continuity Management (BCM) process is critical to the development of successful and robust recovery strategies. In an effort to enhance Business Continuity Management capabilities (and to comply with regulatory guidelines), some corporations have elected to adopt suggested best practices from industry-independent and industry-specific entities and regulatory agencies. Based on our experience and research, a significant (and growing) number of standards exist that are related to BCM. As such, the task of pinpointing best practice consistencies across the majority of these groups can be quite daunting.

After studying the various recommended and mandatory BCM guidelines, we were able to identify common themes and specific process steps that will help in the implementation of a successful BCM process. Below is our list of BCM standards and the associated agencies that advocate each best practice:

Business Continuity Plan Component/Task	NFPA National Fire Protection Agency	FEMA Federal Emergency Management Association	COBIT Control Objectives for Information and Related Technologies	NIST National Institute of Standards & Technology	FFIEC Federal Financial Institutions Examination Council	FED Federal Reserve Board	HIPAA Health Insurance Portability & Accountability Act	FERC Federal Energy Regulatory Commission	DRI Disaster Recovery Institute
Process Management									
Institute a BCM process that includes crisis management, business resumption planning, and IT recovery	√	√	√	√	√				√
Establish a BCM steering committee that includes a coordinator and others who have both operations and technology expertise	√	√		√	√				√
Define BCM objectives	√	√		√	√				√
Document a BCM Mission Statement	√	√		√					√
Schedule and document BCM testing and maintenance events		√		√	√				√
Conduct a Risk Assessment									
Identify key legislation, insurance, regulations and industry codes of practice	√	√	√		√	√	√		√

Business Continuity Plan Component/Task	NFPA National Fire Protection Agency	FEMA Federal Emergency Management Association	COBIT Control Objectives for Information and Related Technologies	NIST National Institute of Standards & Technology	FFIEC Federal Financial Institutions Examination Council	FED Federal Reserve Board	HIPAA Health Insurance Portability & Accountability Act	FERC Federal Energy Regulatory Commission	DRI Disaster Recovery Institute
Define a formal, risk assessment process with the objective of identifying the source, likelihood and vulnerability of specific threats that may affect operations	√	√		√	√		√		√
Assess current mitigating controls	√	√		√	√		√		√
Conduct a Business Impact Analysis									
Identify key business processes and critical dependencies; the impacts of potential business interruptions should be identified and continually updated	√	√		√	√	√	√		√
Identify process-specific Recovery Time Objectives (RTO)	√	√	√	√	√	√			√
Identify minimum capacity requirements to restore business operations to an acceptable level	√	√	√	√	√	√		√	√
Prioritize recovery efforts based on established RTOs	√	√	√	√		√			√
Review Service Level Agreements between the organization and its external partners	√	√	√		√	√	√		√
Identify and catalog critical resources, records, facilities, equipment, vital records, critical data and infrastructure	√	√	√	√	√	√	√	√	√
Define Recovery Strategies									
Establish a procedure for contracting with vendors should be established in order to acquire critical resources in the event of a disaster	√	√	√	√	√	√	√		√
Identify and document contact information and procedures for local authorities	√	√	√		√	√			√

Business Continuity Plan Component/Task	NFPA National Fire Protection Agency	FEMA Federal Emergency Management Association	COBIT Control Objectives for Information and Related Technologies	NIST National Institute of Standards & Technology	FFIEC Federal Financial Institutions Examination Council	FED Federal Reserve Board	HIPAA Health Insurance Portability & Accountability Act	FERC Federal Energy Regulatory Commission	DRI Disaster Recovery Institute
Identify alternate recovery site(s) for all critical business processes	√	√	√	√	√	√	√		√
Conduct a cost benefit analysis to determine the location and costs associated with recovery site alternatives and the distance from the primary site	√	√	√	√	√				√
Define Business Continuity Management Procedures									
Standard methods for documenting response, recovery and restoration procedures, communication plans, etc.	√	√	√	√	√			√	√
Develop and document procedures for relocating and recovering critical business processes based on management-approved recovery time objectives	√	√	√	√	√	√	√		√
Document emergency response and business/IT process recovery procedures that are - team-based - checklist oriented - chronological	√	√	√	√					√
Define the names of emergency response and recovery team members, together with their contact information	√	√	√	√	√	√		√	√
Create response, recovery and restoration activities that take into account personnel safety and physical and IT security	√	√	√	√	√	√	√	√	√
Document crisis communication procedures	√	√	√	√		√			√
Identify a crisis communications coordinator should be identified	√	√		√					√
Training and Awareness Plan									

Business Continuity Plan Component/Task	NFPA National Fire Protection Agency	FEMA Federal Emergency Management Association	COBIT Control Objectives for Information and Related Technologies	NIST National Institute of Standards & Technology	FFIEC Federal Financial Institutions Examination Council	FED Federal Reserve Board	HIPAA Health Insurance Portability & Accountability Act	FERC Federal Energy Regulatory Commission	DRI Disaster Recovery Institute
Develop and document training plans; training should occur on a regular, defined basis	√	√	√	√	√	√	√		√
Plan Testing Procedures									
Assign, document, and communicate roles and responsibilities for BCP testing; tests should involve all critical business units, departments and functions.	√	√	√	√	√	√	√	√	√
Utilize numerous types of testing approaches (table top drills, disaster simulations and full plan tests)	√	√	√	√	√				√
Implement a post-test analysis report and review process	√	√	√	√	√	√			√
Auditing and Maintaining the Plan									
Define and document specific timelines for updating the business continuity plan	√	√	√	√	√				√
Store the BCP both online and off-site	√	√	√	√	√				√
Audit the BCM process on a periodic basis to ensure compliance with company standards	√	√	√	√	√	√	√	√	√

Although these governing authorities agree on a majority of the recommendations, some best practices were omitted from a majority of the published regulations. To summarize, the following “gaps” should not be overlooked when developing and implementing a Business Continuity Management process.

- A BCP Budget should be formalized and approved by senior management
- Formal disaster declaration authorities, which will be responsible for implementing the continuity strategies in the event of a disaster or business interruption, should be identified.
- The organization should implement an incident management system or process for stabilizing, monitoring, and recovering from a disaster or business interruption.
- The plan should be reviewed periodically and benchmarked against industry regulations and other organizations' processes.

Regardless of the maturity of your organization’s Business Continuity Management process, regulations and guidelines are an excellent approach to ensure completeness and compliance with best practices. Through compliance with these guidelines, your company can help to ensure a comprehensive business continuity management process.

Brian Zawada (CBCP), a Senior Manager and the firm’s Business Continuity Management product leader, is located in Protiviti’s Cleveland office. Brian can be reached at brian.zawada@protiviti.com. Jared Schwartz (CBCP) is a Senior Consultant and is located in New York’s Manhattan office. Jared can be reached at jared.schwartz@protiviti.com. Both Brian and Jared specialize in the development and implementation of BCM solutions nationwide.

This white paper was contributed by KnowledgeLeader, a website providing tools, templates, and other resources for internal audit and risk management professionals. The KnowledgeLeader Internal Audit and Risk Management Community is designed to help companies stay up-to-date on current internal audit, business and technology risk issues, and to become more efficient and effective. The service is provided by Protiviti, an independent firm dedicated exclusively to risk consulting and internal audit.

For more information, see <http://www.knowledgeleader.com/>.

For questions please telephone: 1 866 923 8513. For requests from outside the U.S. or Canada, call +1 925 598 7771.

Material from the KnowledgeLeader® Internal Audit and Risk Management Community

<http://www.knowledgeleader.com>

© 2003 Protiviti. All right reserved.