



Recent Business Continuity Planning (BCP) Regulations, Audit, Governance and Compliance Issues

Association of Contingency Planners – Orange
County Chapter

January 14, 2009

 **ERNST & YOUNG**
Quality In Everything We Do

Anticipated Meeting Outcomes

- ▶ BCP Regulations and Standards:
 - ▶ Why are they important?
 - ▶ What are some commonly used or referred to?
 - ▶ Why do they contain?
 - ▶ Sample minimum requirements
- ▶ BCP Regulations and Standards Comparative Analysis
- ▶ Some Recent changes in BCP Regulations and Standards
- ▶ Evolution of BCP Regulations and Standards: Trends
- ▶ Regulation vs. Standard
- ▶ BCP Program Development: How to determine which regulation/ standard to use?
- ▶ Issues/challenges faced when working with BCP Regulations and Standards
- ▶ Audit, Governance and Compliance
- ▶ BCP Regulations and Standards: Ernst & Young's Experience
- ▶ Summary - Business Continuity Planning Industry Regulations and Standards
- ▶ Provide Helpful Online Resource Links

BCP Regulations and Standards: Why are they important?

- ▶ It is the law - BCP is becoming increasingly regulated in many industries, such as:
 - ▶ Financial services
 - ▶ Healthcare
 - ▶ Government agencies
- ▶ Huge disasters (9/11, tsunami, recent hurricanes, fires, blackouts, etc) highlight the BCP/DRP requirement
- ▶ There are high availability business requirements that critical data and systems be available at all times
- ▶ Various penalties may be imposed on the organizations, if BCP/DRP are not implemented per the requirements:
 - ▶ Securities and Exchange Act, Sections 32(a) and (b) require organizations to protect computerized information; document process used to assess risks of information loss; exercise “duty of care” – Potential fines imposed include personal fines up to \$10,000 and corporate fines up to \$1,000,000.
 - ▶ Penalties may also result due to delays in critical business process deadlines

BCP Regulations and Standards: What are some commonly used/referred to?

- ▶ National Fire Protection Association: “NFPA 1600: Standard on Disaster/Emergency Management and BCP”
- ▶ British Standards: BS 25999 – Business Continuity Management Codes and Specifications
- ▶ ISO standard
 - ▶ ISO/PAS 22399: Incident preparedness and operational continuity management
 - ▶ ISO 17799: Component - Business Continuity Management
 - ▶ ISO/IEC 24762:2008, Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services
- ▶ Federal Financial Institutions Examination Council (FFIEC): FFIEC BCP Examiners Handbook
- ▶ New York Stock Exchange (NYSE) Rule 446
- ▶ The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- ▶ The National Association of Security Dealers (NASD) rules 3510 and 3520
- ▶ Securities and Exchange Act, Sections 32(a) and (b)
- ▶ IT Infrastructure Library (ITIL) guidelines for the business continuity planning process and documentation.
- ▶ North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) requirements: NERC CIP-009-1
- ▶ ASIS International Organizational Resilience: Preparedness and Continuity Management (Leading Practices only) The Disaster Recovery Institute International (DRII): “Business Continuity Planning Professional Practices”
- ▶ (Leading Practices only) The Business Continuity Institute (BCI): “Business Continuity Management: Good Practice Guidelines”

BCP Regulations and Standards: What do they contain?

Minimum requirements on one or more of the following:

- ▶ Policy and Program Management
- ▶ Threat & Risk Assessment
- ▶ Mitigation & Emergency Preparedness
- ▶ Business Impact Analysis
- ▶ Recovery Strategy Development
- ▶ Business Continuity Planning
- ▶ Disaster Recovery Planning
- ▶ Crisis/Incident Management
- ▶ Training
- ▶ Testing & Validation
- ▶ Maintenance

BCP Regulations and Standards: Sample Minimum Requirements

- ▶ Comprehensive BIA and risk assessment
- ▶ Identification of all mission-critical systems and backup for such systems
- ▶ Alternate internal and external communications
- ▶ Hard copy and/or electronic backup and recovery for vital records, as required
- ▶ Alternate workspace strategies
- ▶ Succession planning to help ensure that the leadership will continue to function effectively under emergency conditions
- ▶ Compliance with applicable legislation, policies, regulatory requirements, and directives.
- ▶ Communications with regulators.
- ▶ Regular updates to the BCP based on changes in business processes, audit recommendations, and lessons learned from testing

BCP Regulations and Standards: Comparative Analysis - *Examples*

Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Requires that customers are able to switch between health insurance providers as smoothly as possible without unavailability, total loss, or loss of integrity of their health data, dictates that organizations must have a contingency plan in place in order to conform to the Act.
The National Association of Security Dealers (NASD) rules 3510 and 3520 (2004)	Require that all members have a Business Continuity Plan in place and provide emergency contact information
ISO 17799	Requires business continuity and disaster recovery plans to be in place.
FFIEC IT Handbook – Business Continuity Planning (2008)	Focuses on the need for enterprise-wide business continuity planning for all in-house and serviced activities (FFIEC is specific to financial institutions)
SEC regulations (for example, SEC 17 CFR 240)	Require that financial transaction histories be maintained for all electronic securities transactions, and backup power be in place to maintain continuity.
Basel II	Requires accurate maintenance of historical transaction data and continuous availability of all components of distributed financial systems involved in the Bank of International Settlements (BIS) systems.
NFPA 1600 (2007)	Requires that the measures that are taken to protect the vital records (i.e. financial data, personnel records, etc.)

Some Recent changes in BCP Regulations and Standards

- ▶ FFIEC, Latest update:2008
 - ▶ Changes focus on management issues, such as:
 - ▶ The need for enterprise-wide involvement in the business continuity planning process
 - ▶ The importance of business continuity planning for all in-house and serviced activities of financial institutions
 - ▶ Lessons learned from financial institutions that suffered damage from Hurricanes Katrina and Rita
 - ▶ Pandemic planning
 - ▶ Overall goal is same as the 2003 version: "...the importance of BCP in establishing the basis for a financial institution's ability to resume operations when the business has been disrupted unexpectedly"
- ▶ NFPA 1600, Latest update: 2007
 - ▶ Changes focus on:
 - ▶ Addition of "Incident Prevention" – Directs the entity to develop a strategy to prevent an incident that threatens people, property and the environment
 - ▶ Includes prevention as part of the planning process, and has a section to address the requirement for the prevention plan
 - ▶ Specifies that organizations conduct this planning process on a regularly scheduled basis or when the situation has changed to put the accuracy of the existing plan into question
 - ▶ Requires that "where applicable, the entity shall include key stakeholders in the planning process."
 - ▶ Overall, the latest version of the standard does not fundamentally alter the purpose of the standard – noted in a documented interview with the Chair of NFPA's Technical Committee on Emergency Management and Business Continuity, Donald L. Schmidt

Some Recent changes in BCP Regulations and Standards

- ▶ NASD rules 3500 series, Filed in 2002 and Effective Latest update: 2004
 - ▶ Amendments require each member to:
 - ▶ Create and maintain a business continuity plan
 - ▶ Identify procedures relating to an emergency or significant business disruption that are “reasonably designed to enable the member to meet its existing obligations to customers”
 - ▶ Address existing relationships with other broker-dealers and counter-parties
 - ▶ Update plan in the event of any material change to operations, structure, business, or location
 - ▶ Designate a member of senior management who is also a registered principal to approve the plan and be responsible for conducting the required annual review
 - ▶ Address how customers will be assured of prompt access to their funds and securities in the event that the member determines it is unable to continue its business.
 - ▶ Make available promptly upon request to the NASD staff
- ▶ NERC CIP-009-1, Latest update: 2006
 - ▶ Changes since NERC 1216 focus on:
 - ▶ The backup and storage of information required to successfully restore Critical Cyber Assets
 - ▶ Definition of the roles and responsibilities of responders
 - ▶ Update of recover plans after each exercise
 - ▶ Annual test of Information essential to recovery stored on backup media
 - ▶ Overall, there are some new additional requirements since NERC 1216. However, for the most part, more specificity has been detailed on the requirements in the new NERC CIP-009-1

Evolution of BCP Regulations and Standards: Trends

- ▶ BCP Regulations and Standards have become more stringent and specified
- ▶ Overall goals have remained the same
- ▶ Updates reflect lessons learned from major disasters
- ▶ Updates reflect higher-level of customer/client expectations
- ▶ Updates reflect greater demands of business uptime and timely disaster response
- ▶ Making a transition from more “guidelines and standards” documentation to “regulations and laws” – (BCP is not just a “nice to have” anymore; it is a requirement by the law)
- ▶ Making the process more clearly auditable and certifiable

Regulations vs. Standards

▶ Regulations

- ▶ “...are mandatory authoritative rules dealing with details or procedures having the force of law, which are issued by and authority of government”
- ▶ Examples: SEC - NASD, FFIEC, HIPPA

▶ Standards

- ▶ “...are a setup of voluntary criteria, voluntary guidelines and best practices used to enhance the quality, performance, reliability, and consistency of products, services and/or processes”
- ▶ Examples: NFPA 1600, ISO/PAS 22399, ASIS International Organizational Resilience: Preparedness and Continuity Management – Best Practices Standard, BS 25999-2, NERC CIP-009-1

BCP Program Development: How to determine which regulations or standard to use?

- ▶ Most regulations are specific to an industry or a membership of a company in a particular commission or entity. For example:
 - ▶ FFIEC: Applies to financial institutions
 - ▶ NYSE: Applies to NASD and NYSE members
- ▶ See if your company falls under the requirement of any BCP regulations
- ▶ Standards represent different focuses:
 - ▶ NERC Standards: focused on recovery planning related to cyber security
 - ▶ ISO/IEC 24762:2008: focused on Information technology–Guidelines for information and communications technology disaster recovery services
- ▶ Multiple standards can be referred to during BCP program development, depending on the particular area being addressed
- ▶ There are standards and leading practices that cover overall business continuity development and management without any single/specific focus, such as:
 - ▶ British Standards: BS 25999
 - ▶ The Disaster Recovery Institute International (DRII): “Business Continuity Planning Professional Practices”

Issues/challenges faced when working with BCP Standards and Regulations

- ▶ The challenge of keeping up with modifications to standards and regulations
- ▶ Auditing specifically against a standard or regulation: Not all are easily auditable
- ▶ Certifying that your program meets the guidance/requirements laid out by a standard/regulation: Not all are currently certifiable
- ▶ Expectations of customers/clients/third-party partners to meet specific standards and/or regulations

Audit, Governance and Compliance

- ▶ Examples of requirements of a BCP Audit:
 - ▶ COBIT audits require a BCP to be in place and to be effective in order to meet compliance requirements
 - ▶ Business continuity and disaster recovery plans are a key component of any ISACA audit
- ▶ Examples of certifications
 - ▶ BS 25999 certification
 - ▶ Dept of Homeland Security - Private Sector Certification (under development)
 - ▶ Title IX of H.R. 1 And Public Law 110-53
 - ▶ Implementing Recommendations of the 9/11 Commission Act of 2007
- ▶ BCP is a “live” program and per numerous standards and regulations, should be assessed and updated at least annually
 - ▶ Conduct Annual Current State Assessments
 - ▶ Integrate BCP/DRP audit in your annual internal audits

BCP Regulations and Standards: Ernst & Young's Experience

- ▶ Helped organizations develop BCP program per the requirements laid out by multiple BCP Regulations and Standards. Provided assistance in one or more of the following:
 - ▶ Policy and Framework Development
 - ▶ Threat and Risk Assessment and Business Impact Analysis
 - ▶ Emergency Preparedness
 - ▶ Crisis/Incident Management Planning
 - ▶ Workspace and IT Recovery Strategies Development
 - ▶ Business Continuity and Disaster Recovery Planning
 - ▶ Testing, Maintenance, Program Awareness
- ▶ Created audit programs and tools to help audit against a particular/multiple regulation(s)
- ▶ Worked with clients to help assess and maintain their BCP program per the guidelines/requirements laid out in various BCP Regulations and Standards
- ▶ Conducted current state reviews of BCP programs in comparison to BCP leading practices
- ▶ EY BCP Fact: Ernst & Young has a fully dedicated and experienced business continuity planning practice with over 150 BCP advisors globally
- ▶ EY BCP Focus: Consistent focus on business value and business risk

Summary - Business Continuity Planning Industry Regulations and Standards

- ▶ Business continuity standards are getting more attention than ever before
- ▶ There is no single accepted standard
- ▶ The interest in standards and certification will continue to grow
- ▶ There will be increasing expectations of your customers/clients and business partners to meet the standards

Helpful Resources - Business Continuity Planning Industry Regulations and Standards

- ▶ FFIEC BCP Booklet:
http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#bcp
- ▶ NFPA 1600:
<http://www.nfpa.org/assets/files/PDF/NFPA1600.pdf>
- ▶ NASD Rules 3510 and 3520
<http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p003095.pdf>
- ▶ BS 25999
<http://www.bsi-global.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/BS-25999/>
- ▶ NERC CIP-009-1
<http://www.nerc.com/files/CIP-009-1.pdf>
- ▶ NYSE Rule 446
[http://apps.nyse.com/commdata/PubInfoMemos.nsf/AllPublishedInfoMemosNyseCom/85256A71006FB86385256E84006B652D/\\$FILE/Microsoft%20Word%20-%20Document%20in%2004-24.pdf](http://apps.nyse.com/commdata/PubInfoMemos.nsf/AllPublishedInfoMemosNyseCom/85256A71006FB86385256E84006B652D/$FILE/Microsoft%20Word%20-%20Document%20in%2004-24.pdf)

Contact Information

Anupama (Anu) Sahni

Senior Manager
+1 949 437 0724
anupama.sahni@ey.com

- ▶ Anu has over eight years of experience advising companies on business continuity planning and disaster recovery planning and is CISSP-certified.
- ▶ Anu has co-facilitated large BCP exercise sessions, including a 200-participant session at an international BCP conference and been a speaker at professional organization lunch events.
- ▶ She is knowledgeable on multiple tools and has developed and provided in-depth training on multiple tools.
- ▶ Anu has experience leading various BCP activities including current state review, business impact assessment, risk assessment, process model design, strategy development, crisis management planning, business continuity planning, disaster recovery planning and BCP benchmarking.
- ▶ She has co-authored a white paper on Pandemic Business Continuity Planning.