

---

## U.S. Regulatory Climate.

### “REGULATIONS THAT INFLUENCE

the Business Continuity and Disaster Recovery industry.”

---

#### Understanding the Law

Understanding the laws and regulations that impact Business Continuity and Disaster Recovery planning in an important first step. While regulatory compliance may be a driving factor within many organizations we can also leverage our Business Continuity and Disaster Recovery initiatives to generate immediate return on our efforts.

#### These are Numerous Laws and Regulations:

- Regulations that apply to all industries
- Financial Regulations
- Healthcare Regulations
- Government Agency Regulations
- Utilities Regulations
- International Organization for Standardization (ISO)

---

“Even if BC/DR is not specified in a law or regulation, issues of data integrity, availability and internal controls do impact your BC/DR

## Initiatives.”

---

#### Standards and Regulations:

There are essentially two different types of regulatory compliance. First, there are standards and requirements that need to be met in order to become a member of an organization. Some examples of such organizations are the ISO and the FDIC.

Then there are government regulations that are imposed upon specific industries, which mandate that in order to do business in that industry, our organization must comply. These regulations are created for the good of the people and create national standards of uniformity.

Most regulations are mandated for the purposes of standardization, the ability to respond effectively to disaster, information security and ensured continuity of business practices, as well as a few that make board members accountable. A good example of this is the Sarbanes-Oxley Act of 2002, which pertains to all publicly held companies.

According to the American Management Association, “**About 50% of business that suffer from a major disaster without a disaster recovery plan in place never reopen for business.**” The Sarbanes-Oxley Act (SOX) increased a Corporate Officer’s liability for business continuity. Section 404 of the Act is about Internal Controls and is material to financial reporting. In order to determine whether something is subject to these controls, companies must perform a Business/Application Value Assessment, commonly referred to as a Business Impact Analysis.

SOX Section 406 (c)(2) requires “full, fair, accurate, timely, and understandable disclosure in the periodic reports required to be filed by the issuer.” Essentially, a BC/DR (Business Continuity and Disaster Recovery) plan determines how a company will comply with this section.

Industry	Regulation	BC/DR Impact	Key Notes
All Industries	Sarbanes-Oxley Act	Specifies that Corporate Officers are liable for Business Continuity	Pertains to Publicly held companies in the US
All Industries	IRS Procedure 86-19	Requires off-site protection and documentation of computer records maintaining tax info	Records must be available in the event that the primary facility is unable
All Industries	Consumer Credit Protection Act (CCPA) Section 2001 Title 1X	Due Diligence for availability of data in Electronic Funds Transfers including Point of Sale	
All Industries	Foreign Corrupt Practices Act 1977	Requires that publicly-held corporations provide "reasonable protection for IT systems"	Holds Management accountable

Industry	Regulation	BC/DR Impact	Key Notes
Healthcare	Health Insurance Portability & Accountability Act (HIPAA) 1996	Requires data backup plan, DR plan and emergency mode operations plans	Requirements correlate to Business Continuity Plan
Healthcare	Food and Drug Administration (FDA) Code of Federal Regulations (CFR), Title XXI, 1999	Requires BC measures to ensure availability of information	Establishes the requirements for electronic records and electronic signatures

Industry	Regulation	BC/DR Impact	Key Notes
Financial	Gramm-Leach-Bliley Act 1999	Institutions are required to implement a written information security program that includes: Admin, technical and physical safeguards	Requirements correlate to Business Continuity Plan
Financial	Federal Financial Institutions Examination Council (FFIEC)	Specifies that Board of Directors is responsible for ensuring that a comprehensive BC plan has been implemented	
Financial	BASEL II, Basel Committee on Banking Supervision 2003	Requires that banks put in place BC/DR plans to ensure continuous operations and limit losses	Is a best practice standard as of 2007
Financial	GAO/IMTEC-91-56 Financial Markets: Computer Security Controls	Identified the need for risk assessments, data back up procedures, BC/DR plans to ensure continuous operations and security of US Stock Exchange	Guidelines for stock markets
Financial	FFIEC Inter-Agency Policy 1997	Requires any service bureau or outsourcing companies that service banks have in place BC/DR	
Financial	Expedited Funds Availability (EFA) Act, 1989	Requires federally chartered Financial Institutions to have demonstrable BC/DR Plans	To ensure prompt availability of funds

Industry	Regulation	BC/DR Impact	Key Notes
Government	Continuity of Operations (COOP) and Continuity of Government (COG) Federal Preparedness	Establishes requirements for BC Plans and response readiness.  BC Plans must be able to sustain operations for 30 days	All BC Plans must be maintained at a high level of readiness, must be capable of implementation without warning, must be operational within 12 hours of activation
Government	FEMA FRPG 01-94	All department and agency heads must formally plan for continuity of essential operations	Written documents for Business Continuity must be maintained and current
Government	Federal Information Security Management Act (FISMA) 2002	Requires electronic data to be available during a crisis	Emphasis of FISMA is on data security
Government	National Institute of Standards and Technology (NIST) SP800-34 2002	Requires BC/DR and COOP plans	
Government	NIST 800-53 2005 Recommended Security Controls for Federal Information Systems	Mandatory security controls that have specific requirements for Continuity Planning & testing	Specific details on policy & procedures, plans, training, testing and updating
Government	Governmental Accounting Standards Board (GASB) Statement No. 34 1999	Requires a BC/DR plan to ensure that agency's mission continues in time of crisis	Applies to all government entities that operate utilities

Industry	Regulation	BC/DR Impact	Key Notes
Manufacturing	ISO-9000 Qualifications	Requires Incident preparedness, BC/DR plans, testing and assurances	Operational Continuity Management

Industry	Regulation	BC/DR Impact	Key Notes
Utilities	Federal Energy Regulatory Commission (FERC) RM01-12-00 2003	Mandatory recovery plans	Does not apply to rural utilities service borrowers and limited distribution coops
Utilities	NERC Security Guidelines for Electricity Sector 2001	Includes BC/DR in information security standards for the industry-government partnership	Guided by Critical Infrastructure Protection Committee (CIPC)
Utilities	RUS 7 CFR Part 1730	Emergency restoration plan required for rural utilities	Condition of continued borrowing for Rural Utilities services
Utilities	Presidential Decision Directive 63	Encourages risk management strategies to protect against and mitigate effects of attacks against critical infrastructures and key resources	Applies to interdependent and cyber-supported infrastructures vulnerabilities in both public & private sectors to protect both domestic and international security
Utilities	Presidential Decision Directive 13010	BC/DR Plans required for all National infrastructures	
Utilities	North American Electric Reliability Council (NERC) P6T3	Interim provisions must be included if it is expected to take in excess of 1 hr. to implement primary facilities BC/DR Plan	Specific details on BC/DR plan that include communications, monitoring utilities, training & testing
Utilities	NERC Urgent Action Standard 1216	DR Plans and procedures must be in place, BC Plans are only required for facilities and functions considered "critical"	
Utilities	FTC's - Federal Information Security Management Act 16-CFR-314 2003	FTC's - Federal Information Security Management Act 16-CFR-314 2003	Focus is on security issues, such as password management.
Utilities	Telecommunications Act of 1996, Section 256 Coordination of Interconnectivity	Requires FCC to establish procedures to oversee network planning by carriers and providers.	Recognizes the need for BC/DR plans, does not mandate it
Utilities	TL9000 Section 7.1.C.3	Requires established and maintained BC/DR plans "to ensure the organization's ability to recreate and service the product throughout its life cycle."	Telecom Industry

The International Organization for Standardization (ISO) is administered by accreditation and certification bodies. While the ISO is defined as a non-governmental organization, its history is layered with the proven ability to set standards that often become law, either through treaties or national standards. The ISO generally acts as a consortium with strong links to governments, building consensus between private and public sectors, which makes it more powerful than most non-governmental organizations.

**Some of the requirements of the ISO-9000 standard that also transfer to ITIL® and other Total Quality Management Systems are:**

- Keeping adequate records.
- Implementation of a set of procedures that cover all key processes in the business.
- Continuous monitoring of processes to ensure effectiveness.
- Regularly reviewing individual processes and the quality system itself for effectiveness.
- Implementation of processes for quality controls and facilitating continual improvement.

A good business continuity plan will not only document processes and procedures in a continuous cycle in case of emergency, but also documents the current, business-as-usual procedures for all key processes in the business. The BAM Methodology delivers a complete service method that provides companies with a simple, repeatable and sustainable process for achieving your BC/DR (Business Continuity and Disaster Recovery) goals no matter where you are in your BC/DR efforts.

A great Business Continuity and Disaster Recovery plan will create an index CMDB, Change and Configuration Management, Incident Management, Service Desk, and other base ITIL® capabilities that align to an organizational culture and the context in which it does business.

---

## Re:Think...

compliance. Are we up to date on changes in regulations? Are those regulations being used to boot-strap disaster preparedness at the client's company?

---

## Contact

---

Kevin Burton

kevin@thinkbam.com

480.239.9724

---

Angela McGee

angela@thinkbam.com

480.239.5647