Gartner

Research

Publication Date: 11 July 2005 **ID Number: G00128123**

Laws Influence Business Continuity and Disaster Recovery Planning Among Industries

Kristen Noakes-Fry, Christopher H. Baum, Barry Runyon

A multitude of laws and regulations specify or imply requirements for business continuity and disaster recovery planning. These requirements vary among industry sectors, affecting the development, focus and execution of business continuity plans.

ANALYSIS

What You Need to Know

- Even if business continuity (BC) and disaster recovery (DR) are not specified in a law or regulation, issues of data integrity and availability and internal controls can bring about additional demands for updated BC measures to ensure the continuous availability of information.
- While compliance requires satisfying the letter of the law, BC requires going beyond the minimum requirements, to having in place plans and training — based on industry, geography and business impact analysis (BIA) — to keep your organization going under any circumstances.

Business Continuity and Disaster Recovery

Although a clear organizational boundary exists between the two areas, data security and BC/DR strategies and tactics represent a shared concern because information security risks might well cause an organization to execute its BC/DR plan. Thus, even if a regulation does not specify the kind of business continuity plan (BCP) or how often it must be tested, an organization remains accountable for its systems and processes related to data. The bottom line is that laws and regulations, as well as shareholders, expect organizations to exercise due care to ensure that necessary data is available.

Gartner analysts looked at four industry sectors — healthcare, government, finance and utilities — to determine which laws and regulations most influenced BC/DR in these sectors. Our findings are outlined in Table 1.

Table 1. BC/DR in Healthcare, Government, Finance and Utilities Sectors

Industry Sector	Significant Laws and Regulations	Impact on BCP	Comments
Healthcare	Health Insurance Portability and Accountability Act (HIPAA) of 1996	Requires data backup plan, DR plan and emergency mode operation plan. Requires reasonable and appropriate measures relative to the size, complexity and resources of the organization.	Requires increased budgets, new job descriptions, as well as additional staff and infrastructure. Typically an IT responsibility but may also be the province of the compliance officer or CFO.
	Food and Drug Administration (FDA) Code of Federal Regulations (CFR), Title XXI, 1999	Establishes the requirements for electronic records and electronic signatures.	Acceptability of electronic records and signatures may require that some organizations update their BC measures to ensure the availability of information.

Industry Sector	Significant Laws and Regulations	Impact on BCP	Comments
Government	Federal Information Security Act (FISMA) of 2002, Title III of the E-Government Act of 2002 (PL 107-347, 17 December 2002) Executive Order on Critical Infrastructure Protection in the Information Age, 16 October 2001	Mostly emphasizes data security rather than BC and DR. An important need to be addressed is the requirement that government is open and running during a crisis.	By and large, state and local governments are free to make their own decisions on data security, BR and continuity of operations (COOP).
	COOP and Continuity of Government (COG). Federal Preparedness Circular 69, 26 July 1999	Establishes minimum planning considerations for federal government operations.	BCP must be maintained at a high level of readiness. BCP must be capable of implementation with or without warning. BCP must be operational no more than 12 hours after activation. BCP must maintain sustained operations for up to 30 days. BCP should take maximum advantage of existing agency field infrastructures.
	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Contingency Planning Guide for Information Technology Systems, June 2002	Defines detailed recommendations from NIST, requiring contingency, DR and COOP plans.	Joins the NIST SP 800 series (Parts 3, 4, 12, 14, 16, 18 and now 34) in stating these requirements. Focuses on planning.
	NIST 800-53, Recommended Security Controls for Federal Information Systems, February 2005	Mandatory security controls will become a federal standard by the end of 2005. NIST 800-53A will provide assessment guidelines that are closely aligned to the controls listed in NIST 800-53.	Gives specific requirements for: - Contingency planning policy and procedures - Contingency plan - Contingency training - Contingency plan testing - Contingency plan update
Finance	Federal Financial Institutions Examination Council (FFIEC) Handbook, 2003-2004 (Chapter 10)	Specifies that directors and managers are accountable for organizationwide contingency planning and for "timely resumption of operations in the event of a disaster."	This chapter — on an operational level — supplants many other BCP guidelines. It covers examination requirements for all companies regulated by the Federal Deposit Insurance Corp. (FDIC), Federal Reserve Bank (FRB), Treasury Department, U.S. Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS) and National Credit Union Administration (NCUA).

Industry Sector	Significant Laws and Regulations	Impact on BCP	Comments
	Basel II, Basel Committee on Banking Supervision, Sound Practices for Management and Supervision, 2003	Requires that banks put in place BC and DR plans to ensure continuous operation and to limit losses.	After 2007, influence of Basel II will be limited to about 30 U.S. banks but will spread as a best practice via "audit creep."
	Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, 2003	More focused on systemic risk than individual enterprise recovery. Requires BCPs to be upgraded and tested to incorporate risks discovered as a result of the World Trade Center disaster.	Influences companies that are regulated by Securities and Exchange Commission (SEC), OCC and Board of Governors of the Federal Reserve System (FRS). Authorizes the OCC to take action against banks that fail to comply with requirements for DR by the U.S. financial system.
	Expedited Funds Availability (EFA) Act, 1989	Requires federally chartered financial institutions to have a demonstrable BCP to ensure prompt availability of funds.	
Utilities	Governmental Accounting Standards Board (GASB) Statement No. 34, June 1999	Requires a BCP to ensure that agency mission continues in time of crisis.	Applies to all government entities that operate utilities.
	North American Electric Reliability Council (NERC) 1200 (1216.1), 2003	Recovery plans currently voluntary.	Mandatory obligations pending in the energy bill. NERC 1200 due to be replaced by NERC 1300 by the end of 2005.
	Federal Energy Regulatory Commission (FERC) RM01-12-00 (Appendix G), 2003	Mandates recovery plans.	Does not apply to Rural Utilities Service (RUS) borrowers and limited distribution cooperatives.
	RUS 7 CFR Part 1730, 2005	Emergency restoration plan required as condition of continued borrowing.	Applies to all rural utilities borrowers.
	Telecommunications Act of 1996, Section 256, Coordination for Interconnectivity	Requires the Federal Communications Commission (FCC) to establish procedures to oversee coordinated network planning by carriers and other providers.	While it recognizes the need for DR plans, it also acknowledges the existence of inadequate testing because of the rapid deployment of new technologies.

Industry Sector	Significant Laws and Regulations	Impact on BCP	Comments
	NERC Security Guidelines for the Electricity Sector, June 2001	Includes BC in information security standards for the industry-government partnership (guided by Critical Infrastructure Protection Committee [CIPC]).	

Source: Gartner (July 2005)

Recommendations

- Stay current with the laws and regulations that apply to your particular business sector.
- Note explicit and implicit BCP demands lurking within these regulations.
- Factor in the cost of regulations, such as HIPAA, GASB 34 and FISMA, in every project.
- Seek professional advice to parse the dense and ambiguous language of industry-specific laws and regulations. It will save you money in the long run.
- Try to satisfy more than one law or regulation with each BCP initiative.
- Consider the business continuity management (BCM) guidelines within International Organization for Standardization (ISO) 17799 as a guide for satisfying most federal- and state-mandated BCP requirements.
- Review NIST literature for generally accepted principles and practices in the area of BCP.
- Review NIST Information Technology Laboratory (ITL) publications that address BC planning, implementation, management and operations.
- Use the BCP requirements within industry-specific laws and regulations to gain acceptance of upper management and board. Such acceptance will be helpful in gaining required budget.
- Prioritize enterprisewide responses to industry-specific laws and regulations.
- Be aware of law and regulation violations most often reported and address them sooner rather than later.

Acronym Key and Glossary Terms

BC business continuity

BCP business continuity plan

BCM business continuity management

BIA business impact analysis

CFR Code of Federal Regulations

CIPC Critical Infrastructure Protection Committee

COG Continuity of Government

COOP continuity of operations

DR disaster recovery

EFA Expedited Funds Availability

FCC Federal Communications Commission

FDA Food and Drug Administration

FDIC Federal Deposit Insurance Corp.

FERC Federal Energy Regulatory Commission

FFIEC Federal Financial Institutions Examination Council

FISMA Federal Information Security Act

FRB Federal Reserve Bank

FRS Federal Reserve System

GASB Governmental Accounting Standards Board

HIPAA Health Insurance Portability and Accountability Act

ISO International Organization for Standardization

ITL Information Technology Laboratory

NCUA National Credit Union Administration

NERC North American Electric Reliability Council

NIST National Institute of Standards and Technology

OCC U.S. Office of the Comptroller of the Currency

OTS Office of Thrift Supervision

RUS Rural Utilities Service

SEC Securities and Exchange Commission

SP Special Publication

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner