An Overview of U.S. Regulations Pertaining to Business Continuity

Introduction

Regulatory compliance is a significant factor influencing the development of your business continuity strategy. Moreover, while Business Continuity or Disaster Recovery regulations may not apply in every business situation, a general understanding of legislation governing data integrity, availability and compliance is helpful for any organization developing a Business Continuity strategy.

Essentially, there are two specific types of regulations:

1. Standards and requirements that must be met in order to become a member of an organization (eg. ISO).
2. Government regulations imposed on specific industries which must be adhered to in order to do business. These regulations are created to protect the security of citizens, and create national standards of uniformity.

ALL INDUSTRIES

Regulation	Impact: Business Continuity	Take-Aways
Sarbanes-Oxley Act	Corporate officers are liable for business continuity	Relevant for publicly held companies in the U.S.
IRS Proceedure 86-19	Requires off-site protection and documentation of computer records of tax information	Records must be available in the event that the primary facility is subjected to unplanned outage
Consumer Credit Protection Act (CCPA) Section 2001 Title 1X	Due diligence for availability of data in Electronic Funds Transfers including Point of Sale	
Foreign Corrupt Practices Act 1977	Publicly held corporations must provide “reasonable protection” for IT systems	Holds management accountable

FINANCIAL

Regulation	Impact: Business Continuity	Take-Aways
Expedited Funds Availability (EFA) Act, 1989	Federally chartered financial institutions must have demonstrable business continuity plans	To ensure prompt availability of funds
Gramm-Leach-Bliley Act 1999	Institutions are required to implement a written information security program that includes: admin., tech., and physical safeguards	Requirements related to Business Continuity plan
Federal Financial Institutions Examination Council (FFIEC)	Specifies that Board of Directors is responsible for ensuring that a comprehensive BC plan has been implemented	
BASEL II, BASEL Committee on Banking Supervision 2003	Requires that banks put in place BC?DR plans to ensure continuous operations and limit losses	Best Practice Standard 2007
GAO/IMTEC-91-56 Financial Markets: Computer Security Controls	Outlines the need for risk assessments, data back-up procedures, Business Continuity operations, and security of U.S. Stock Exchanges	Guidelines for stock markets
FFIEC Inter-Agency Policy 1997	Requires any service bureau or outsourcing companies that service banks to have in place	Business Continuity plans

"About 50% of businesses that suffer from a major disaster without a disaster recovery plan in place, never re-open for business."

– American Management Association

HEALTHCARE

Regulation		Impact: Business Continuity	Take-Aways
Health Insurance Portability & Accountability Act (HIPAA 1996)		Requires data back-up plan, disaster recovery emergency plan, and emergency mode operations plans	
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
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
	FEMA FRPG 01-94	All department and agency heads must formally plan for continuity of essential operations	Written documents for BC must be maintained and current
	Federal Information Security Management Act (FISMA) 2002	Requires electronic data to be available during a crisis	Emphasis of FISMA is on data security
	National Institute of Standards and Technology (NIST) SP800-34 2002	Requires electronic data to be available during a crisis	Emphasis of FISMA is on data security
	National Institute of Standards and Technology (NIST) SP800-34 2002	Requires BC/DR and COOP plans	
	NIST 800-53 2005 Recommended security controls for Federal Information systems	Mandatory security controls that have specific requirements for continuity planning and testing	Specific details on policy and procedures, plans, training, testing, and updating
	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 ot all government entities that operate utilities

Utilities	North American Electric Reliability Council (NERC) P6T3	Interim provisions must be included if it is expected to take in excess of 1 hour to implement primary facilities BC/DR Plan	Specific details on BC/DR plan that include communications, monitoring utilities, training and testing
	NERC Urgent Action Standard 1216	DR Plans and procedures must be in place, BC plans are only required for facilities and functions considered "critical."	
	Federal Energy Regulatory Commission (FERC) RM01-12-00 2003	Mandatory Recovery Plans	Does not apply to rural utilities service borrowers and limited distribution co-ops
	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)
	RUS 7 CFR Part 1730	Emergency Restoration Plan required for rural utilities	Condition of continued borrowing for rural utilities services
	Presidential Decision Directive 63	Encourage 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 and private sectors, to protect both domestic and international security
	Presidential decision directive 13010	BD/DR plans required for all national infrastructures	
	FTC's Federal Information Security Management Act 16-CFR-314 2003	Addresses incident Management response and reporting and BC/DR planning	Focus is on security issues, such as password management
	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
	TL9000 Section 7.1.C.3	Requires established and maintained BC/DR plans "to ensure the organizations ability to recreate and service the product throughout its life cycle."	Telecom Industry
Manufacturing	ISO 9000 Qualifications	Requires incident preparedness, BC/DR plans, testing and assurances	Operational Continuity Management