Post 9/11 Surge in Business Continuity Regulations and Standards

1991 - 2001

- Consumer Credit Protection Act
- OMB Circular A-130
- FEMA Guidance Document
- Paperwork Reduction Act
- FFIEC BCP Handbook
- Computer Security Act
- 12 CFR Part 18
- Presidential Decision Directive 67
- FDA Guidance on Computerized Systems used in Clinical Trials
- ANSI/NFPA Standard 1600
- Turnbull Report (UK)
- ANAO Best Practice Guide (Australia)
- SEC Rule 17 a-4

Source: Marsh, (c) 2004

2002 - 2004

- Sarbanes-Oxley Act of 2002
- HIPAA, Final Security Rule
- Fair Credit Reporting Act
- NASD Rule 3510
- NERC Security Guidelines
- FERC Security Standards
- NAIC Standard on BCP
- NIST Contingency Planning Guide
- NYSE Rule 446
- California SB 1386
- Australia Standards BCM Handbook
- GAO Potential Terrorist Attacks Guideline
- Federal and Legislative BC Requirements for IRS
- Basel Capital Accord
- MAS Proposed BCP Guidelines (Singapore)
- NFA Compliance Rule 2-38
- FSA Handbook (UK)
- BCI Standard, PAS 56 (UK)
- Civil Contingencies Bill (UK)
BCP Standards for Financial Institutions

- Federal Financial Institutions Examination Council (FFIEC) BCP Handbook 2003

- SEC Rule 17a  Record Retention Requirements

- NASD Rule 3510

  Rule 3510 will require a business continuity plan that addresses, at a minimum:
  - Data back-up and recovery (hard copy and electronic)
  - Mission critical systems
  - Financial and operational assessments
  - Alternate communications between customers and the firm
  - Alternate communications between the firm and its employees
  - Business constituent, bank and counter-party impact
  - Regulatory reporting
  - Communications with regulators
NYSE Rule 446
(a) Members and member organizations must develop and maintain a written business continuity and contingency plan establishing procedures to be followed in the event of an emergency or significant business disruption. Members and member organizations must make such plan available to the Exchange upon request. (b) Members and member organizations must conduct a yearly review of their business continuity and contingency plan to determine whether any modifications are necessary in light of changes to the member's or member organization's operations, structure, business or location.

National Association of Insurance Commissioners (NAIC)

National Futures Association Compliance Rule 2-38
(a) Each Member must establish and maintain a written business continuity and disaster recovery plan that outlines procedures to be followed in the event of an emergency or significant business disruption. The plan shall be reasonably designed to enable the Member to continue operating, to reestablish operations, or to transfer its business to another Member with minimal disruption to its customers, other Members, and the commodity futures markets. [Adopted effective April 7, 2003.]
BCP Standards for Financial Institutions

- **Uniform Commercial Code**
  - Preparing for foreseeable business disruption

- **Electronic Funds Transfer Act**
  - BCP to meet reasonable standard of care

- **Basel Committee’s Capital Accords and Sound Practices for the Management and Supervision of Operational Risk**

  “Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.”
International Standards

- Australian Standards BCP Guidelines
- Monetary Authority of Singapore BCP Guidelines
- UK: Turnbull Report
- PAS 56
- UK: Financial Services Authority (FSA) Handbook, Ch. 3 Systems & Control
BCP Standards for Non-Financial institutions

- Liability of Corporations
- Liability of Corporate Executives
- Liability to Outside Parties

- Standard of Negligence
  - Standard of Care:
    - Prudent Man Doctrine
    - Exercise same care in managing company affairs as in managing own affairs.

- Informed Business Judgement v. Gross Negligence
Cross-Industry BCP Standards

- Sarbanes-Oxley Act of 2002

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.
(a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—
(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.
(b) INTERNAL CONTROL EVALUATION AND REPORTING.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

- IRS Procedure 86-19

• Requires off-site protection, as well as documentation of computer records maintaining tax information.
Health Insurance Portability and Accountability Act of 1996 (HIPAA), Final Security Rule

7. Contingency Plan (§ 164.308(a)(7)(i))
We proposed that a contingency plan must be in effect for responding to system emergencies. The plan would include an applications and data criticality analysis, a data backup plan, a disaster recovery plan, an emergency mode operation plan, and testing and revision procedures.
In this final rule, we make the implementation specifications for testing and revision procedures and an applications and data criticality analysis addressable, but otherwise require that the contingency features proposed be met.

FDA’s GxP: Good Laboratory Practices

Manufacturing
Clinical
BCP Standards for the Healthcare/Life Science Industries

- **21 CFR Part 11**
  - Audit trails, record retention

- **FDA Guidance on Computerized Systems in Clinical Trials**

  IX. SYSTEM CONTROLS

  B. Contingency Plans

  *Written procedures should describe contingency plans* for continuing the study by alternate means in the event of failure of the computerized system.

  C. Backup and Recovery of Electronic Records

  Backup and recovery procedures should be clearly outlined in the SOPs and be sufficient to protect against data loss. Records should be backed up regularly in a way that would prevent a catastrophic loss and ensure the quality and integrity of the data.
BCP Standards for the Energy Industry

- Federal Electric Reliability Council’s (FERC) Security Standards for Electric Market Participants, July 2002 (draft)

Business Continuity:
Every participant operating a critical electric resource shall have contingency plans that define roles, responsibilities and actions for protecting the rest of the electric grid and market from the failure of its own critical resources. Those plans should further define the roles, responsibilities and actions needed to quickly recover or reestablish electric grid and market functions, processes and systems, in the event that a critical physical or cyber resource fails or suffers harm or attack. Such plans shall be tested or exercised regularly.

- North American Electric Reliability Council’s (NERC) Security Guidelines for the Electricity Sector, June 2002

Continuity of Business Processes:
Reduces the likelihood of prolonged interruptions and enhances prompt resumption of operations when interruptions occur. Consider flexible plans that address key areas such as telecommunications, information technology, customer service centers, facilities security, operations, generation, power delivery, customer remittance and payroll processes. It is useful to revise and test plans on a regular basis. It also is advisable to train personnel so they fully understand their roles with respect to the plans.
IT Standards

- National Institute of Standards and Technology (NIST)
  - *Contingency Planning Guide for Information Technology Systems*

- IT Governance Institute Standards COBIT
  - *Control Objectives for Information and related Technology*

- ISO 17799
Section 6.3.2. Contingency Plans
The organization shall prepare contingency plans to satisfy customer requirements in the event of an emergency such as a utility interruptions, labor shortages, key equipment failure, and field returns.

- **ISO/TS 16949** - Applicable to any supplier to automotive original equipment manufacturer
- **ISO/IEC 17799** - Deals with Information Security

**11 BUSINESS CONTINUITY MANAGEMENT**
11.1 ASPECTS OF BUSINESS CONTINUITY MANAGEMENT
11.1.1 Business continuity management process
11.1.2 Business continuity and impact analysis
11.1.3 Writing and implementing continuity plans
11.1.4 Business continuity planning framework
11.1.5 Testing, maintaining and re-assessing business continuity plans

- **ISO 9001, Quality Management** - Record Retention and Data Availability
- **ISO 14001, Environmental Mgt** - Emergency Preparedness and Response
Meeting the Standards for Disaster Recovery

US v. Carroll Towing Co.

1. Probability of Harm (P): the chance that a damaging event will occur
2. Magnitude of Harm (M): the amount of financial damage that would occur should a disaster happen
3. Cost of Prevention (C): the price of putting in place a means of preventing the disaster’s effects

\[ P \times C = M \]
THANK YOU

www.marshriskconsulting.com