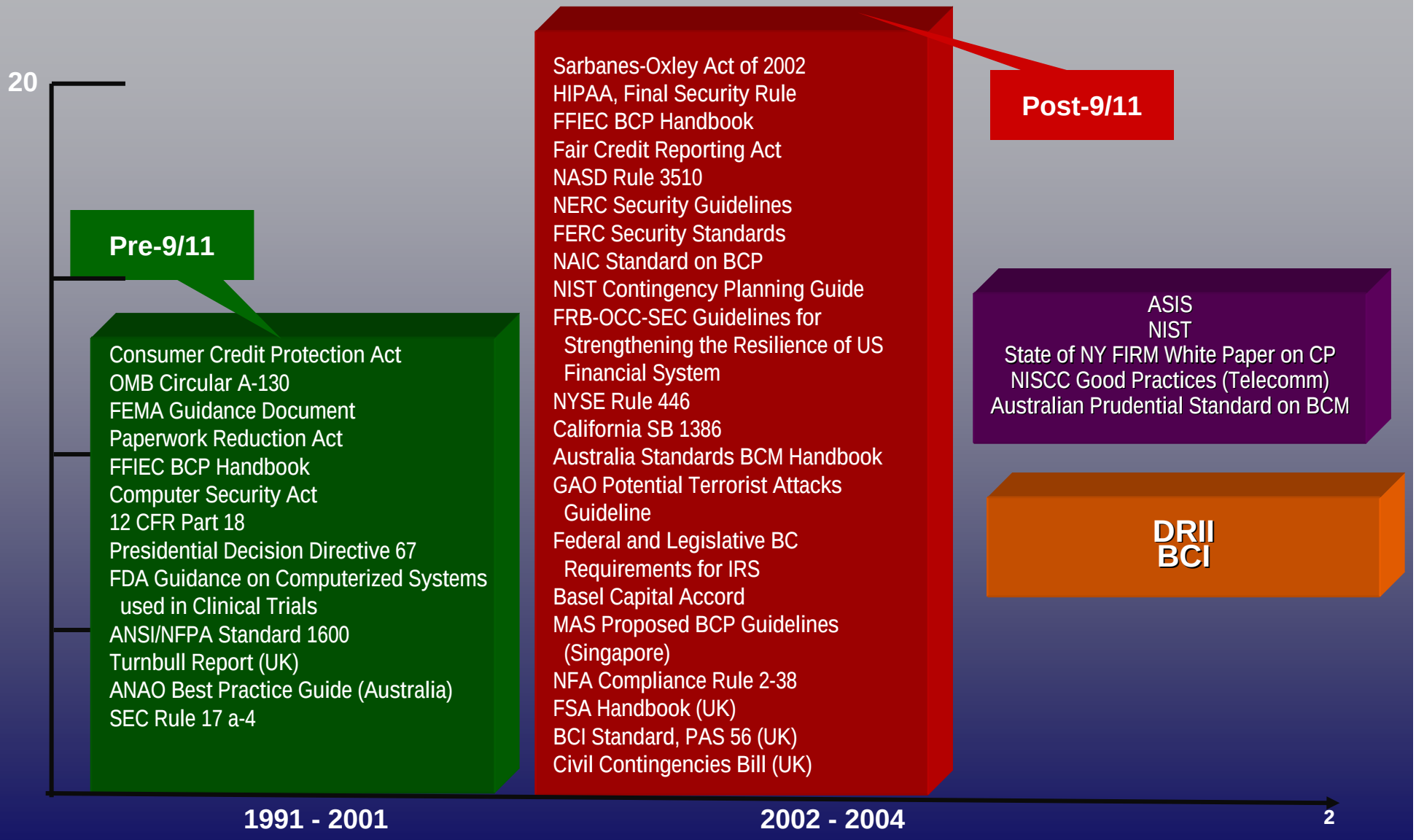
Are You Compliant?

Al Berman

NEDRIX – February 16, 2005

Post-9/11 Surge in Business Continuity Regulations and Standards



BCP Standards for Financial Institutions

- Federal Financial Institutions Examination Council (FFIEC) BCP Handbook 2003 
  - **Business continuity planning is about maintaining, resuming, and recovering the business, not just the recovery of the technology.**
  - **The planning process should be conducted on an enterprise-wide basis.**
  - **A thorough business impact analysis and risk assessment are the foundation of an effective BCP.**
  - **The effectiveness of a BCP can only be validated through testing or practical application.**
  - **The BCP and test results should be subjected to an independent audit and reviewed by the board of directors.**
  - **A BCP should be periodically updated to reflect and respond to changes in the financial institution or its service provider(s).**

BCP Standards for Financial Institutions

- 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

BCP Standards for Financial Institutions

- 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.

BCP Standards for Financial Institutions

- 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."**

BCP Standards for the Healthcare/Life Science Industries

- 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.

HIPAA BCP REQUIREMENTS

Contingency Plan	164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
Emergency Mode Operation Plan			(R)
Testing and Revision Procedure			(A)
Applications and Data Criticality Analysis			(A)

Is it enough ????

BCP Standards for the Healthcare/Life Science Industries

- FDA's GxP: Good **Manufacturing** / **Laboratory** / **Clinical** Practices

- 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.

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.

IS THERE BCP IN SARBANES-OXLEY????

Is There BCP in Sarbanes-Oxley?

- PCAOB (Public Company Accounting Oversight Board)

NO

"Furthermore, management's plans that could potentially affect financial reporting in future periods are not controls. For example, a company's business continuity or contingency planning has no effect on the company's current abilities to initiate, authorize, record, process, or report financial data.

Therefore, a company's business continuity or contingency planning is not part of internal control over financial reporting."

Is There BCP in Sarbanes-Oxley?

- Practitioners

  YES

Are They A Client?

- FFIEC – Appendix D - Interdependencies

  -**THIRD-PARTY PROVIDERS, KEY SUPPLIERS, AND BUSINESS PARTNERS**

    -**outsourcing information, transaction processing, and settlement activities**

      -**Institutions should review and understand service providers' BCPs and ensure critical services can be restored within acceptable timeframes based upon the needs of the institution**

MANUFACTURE AND PRINTING OF CHECKS???

Are They A Client?

- HIPAA – Business Associate (aka Chain of Trust)

  –the business associate must--(1) implement safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity; (2) ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate safeguards;

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

Standards

- **Uniform Commercial Code**
  - Preparing for foreseeable business disruption
- 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 Standards and Business Continuity

- ISO/TS 16949 - Applicable to any supplier to automotive original equipment manufacturer

  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/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**

Is It BCP?

Business Continuity vs.Vital Records

- Foreign Corrupt Practices Act – "Make and keep records and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets."

- SEC Rule 17a - Record Retention Requirements

- IRS Procedure 86-19 - Requires off-site protection, as well as documentation of computer records maintaining tax information.

Legal Standards

- 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

Case Law – Legal Precedence

- **Blake *v.* Woodford Bank & Trust Co. (1977)** – Foreseeable workload – failure to prepare
- **Sun Cattle Company, Inc.*vs.* Miners Bank (1974)** – Computer System Failure – Foreseeable Computer Failure
- **Uniform Commercial Code** – Preparing for foreseeable business disruption

Meeting the Standards

US v. Carroll Towing Co. (1947)

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 * C = M

Thank You

Statements concerning legal matters should be understood to be general observations based solely on our experience as risk consultants and should not be relied upon as legal advice, which we are not authorized to provide. All such matters should be reviewed with your own qualified legal advisors in these areas.