IT Service Delivery And Support Week Nine - BCP

IT Auditing and Cyber Security

Fall 2016

Instructor: Liang Yao

Business Continuity Planning Process

- Samples of Recent Catastrophic Events
- Objectives
- Key BCP Steps
- BCP Development
- BCP Testing Principles
- Other Related Policies, Standards and Processes
- Pandemic
- BCP Audit Program

Morgan Stanley Case

- *“During the first World Trade Center attack in 1993, Morgan Stanley (MS) learned an important lesson. None of the MS employees lost their lives, but it took four hours for all of the employees to evacuate the building. As a result, management decided that the BCP needed to be updated. MS took a careful look at its business operations and the risk of potential disasters and developed a new plan. On Sept. 11, 2001, the planning paid off. After the first hijacked plane slammed into the first World Trade Center tower, MS security evacuated all the employees. The evacuation took only 45 minutes this time, allowing MS to get on with recovering daily operations. Improvements to ER capabilities likely saved numerous lives. The BCM capabilities were also improved as part of the review.” – GTAG Business Continuity Management*

BCP Objectives

- The business continuity planning process should include the recovery, resumption, and maintenance of all aspects of the business, not just recovery of the technology components;
- Business continuity planning involves the development of an enterprise-wide BCP and the prioritization of business objectives and critical operations that are essential for recovery;
- Business continuity planning should include regular updates to the BCP based on changes in business processes, audit recommendations, and lessons learned from testing; and
- Business continuity planning represents a cyclical, process-oriented approach that includes a business impact analysis (BIA), a risk assessment, risk management, and risk monitoring and testing.

BCP Objectives

- The business continuity planning process should include the recovery, resumption, and maintenance of all aspects of the business, not just recovery of the technology components;
- Business continuity planning involves the development of an enterprise-wide BCP and the prioritization of business objectives and critical operations that are essential for recovery;
- Business continuity planning should include regular updates to the BCP based on changes in business processes, audit recommendations, and lessons learned from testing; and
- Business continuity planning represents a cyclical, process-oriented approach that includes a business impact analysis (BIA), a risk assessment, risk management, and risk monitoring and testing.

Key BCP Steps:

- Business Impact Analysis
- Risk assessment
- Risk management
- Risk monitoring and testing

Business Impact Analysis (BIA)

- Assessment and prioritization of all business functions and processes, including their interdependencies, as part of a work flow analysis;
- Identification of the potential impact of business disruptions resulting from uncontrolled, non-specific events on the institution's business functions and processes;
- Identification of the legal and regulatory requirements for the institution's business functions and processes;
- Estimation of maximum allowable downtime, as well as the acceptable level of losses, associated with the institution's business functions and processes; and
- Estimation of recovery time objectives (RTOs), recovery point objectives (RPOs), and recovery of the critical path.

Business Impact Analysis (BIA)

Sample Business Impact

- Health and safety (e.g., injury).
- Environmental (e.g., spill).
- Customer service (e.g., loss of customers).
- Financial (e.g., penalties).
- Regulatory/legal (e.g., governmental action).
- Reputation (e.g., loss of image).

Business Impact Analysis (BIA) Sample Questions:

- What critical interdependencies exist between internal systems, applications, business processes, and departments?
- What specialized equipment is required and how is it used?
- How would the department function if the mainframe, network and/or Internet access were not available?
- What single points of failure exist and how significant are those risks?
- What are the critical outsourced relationships and dependencies?
- What are the required responsibilities of the institution and the third-party service provider as defined by the service level agreement?

Business Impact Analysis (BIA) Sample Questions (cont.)

- What critical operational or security controls require implementation prior to recovery?
- What is the minimum number of staff and amount of space that would be required at a recovery site?
- What special forms or supplies would be needed at a recovery site?
- What equipment would be needed at a recovery site to communicate with employees, vendors, and customers?
- What is the potential impact if common recovery sites serve multiple financial institutions?
- Have employees received cross training, and has the department defined back-up functions/roles that employees should perform if key personnel are not available?
- Are the personal needs of employees adequately considered?
- What are the critical cash management/liquidity issues?

Risk Assessment

- Evaluating the BIA assumptions using various threat scenarios;
- Analyzing threats based upon the impact to the institution, its customers, and the financial market it serves;
- Prioritizing potential business disruptions based upon their severity, which is determined by their impact on operations and the probability of occurrence; and
- Performing a "gap analysis" that compares the existing BCP to the policies and procedures that should be implemented based on prioritized disruptions identified and their resulting impact on the institution.

Common Disaster Scenarios

- Fire
  - 4,000 US citizens die and more than 20,000 injured because of fire
  - Property loss: over $10 billon a year
- Pandemic
  - Global disease outbreak
  - Little or no immunity
  - Economic impact and government regulation
- Terrorism
  - Public fear
  - To prove government is powerless
  - Form of terrorism threats

Common Disaster Scenarios

- Biological Attacks
  - Biological agents – anthrax
  - Virus
  - Chemical
- Tornadoes
- Hurricanes/Typhoons
- Flooding
- Cyber Threats

Impact of Disruptive Events

- **Geographic extent of the impact:** A single building (e.g., fire), entire facility complex (e.g., chemical spill), metropolitan area (e.g., transportation strike), large region (e.g., earthquake), or potentially the world (e.g., pandemic flu).
- **Days of impact:** Number of days before operations will likely return to 75 percent functionality, which means 75 percent of people, resources, and production are functioning. Days of impact may be the period before the organization can replace lost resources, like renting a new building and making it functional after a building fire.
- **Availability of staff (by days):** Percentage of staff that likely would be able to work based on each likely disaster event (by days: 0, 3, 7, 14, or 30). Staff may need to go home for an extended period for some disasters like earthquakes that may damage homes.
- **Availability of operations and/or offices:** Likely percentage of operations and/or office space that is functional (during the days of impact).
- **Availability of IT (during the days of impact):** Likely availability of key IT components for each disaster event. This includes IT infrastructure (logon capabilities), IT network, IT applications, etc.

Business Continuity Plan Development

BCP Development

- Based on a comprehensive BIA and risk assessment;
- Documented in a written program;
- Reviewed and approved by the board and senior management at least annually;
- Disseminated to company employees;
- Properly managed when the maintenance and development of the BCP is outsourced to a third-party;

Business Continuity Plan Development

- Specific regarding what conditions should prompt implementation of the plan and the process for invoking the BCP;
- Specific regarding what immediate steps should be taken during a disruption;
- Flexible to respond to unanticipated threat scenarios and changing internal conditions;
- Focused on the impact of various threats that could potentially disrupt operations rather than on specific events;
- Developed based on valid assumptions and an analysis of interdependencies; and
- Effective in minimizing service disruptions and financial loss through the implementation of mitigation strategies.

Business Continuity Plan Development (cont.)

- Assumptions/Scenarios:
  - Critical personnel are unavailable and they cannot be contacted;
  - Critical buildings, facilities, or geographic regions are not accessible;
  - Equipment (hardware) has malfunctioned or is destroyed;
  - Software and data are not accessible or are corrupted;
  - Third-party services are not available;
  - Utilities are not available (power, telecommunications, etc.);
  - Liquidity needs cannot be met; and
  - Vital records are not available
  - IT systems

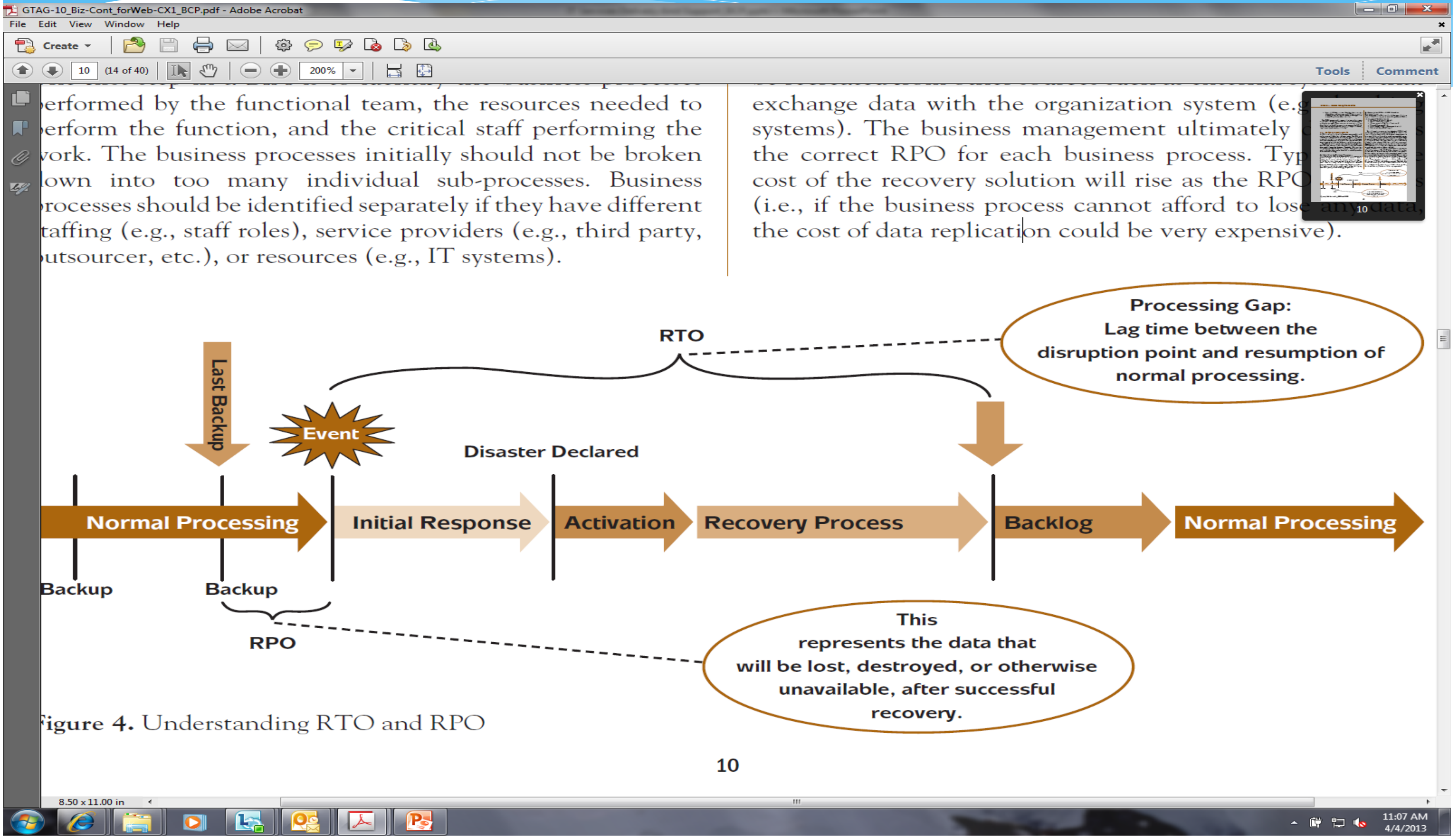
Business Continuity Plan Development (cont.):

- Mitigation Strategies
  - Strengthening the physical facility using dependable construction materials;
  - Establishing redundant vendor support;
  - Establishing media protection safeguards and comprehensive data back-up procedures;
  - Implementing redundant or alternative power sources, communication links, data back-up technologies, and data recovery methods;
  - Increasing inventories of critical equipment;
  - Installing fire detection and suppression systems; and
  - Purchasing and maintaining adequate reserves of food, water, batteries, and medical supplies.

Business Continuity Strategy

- **Manual work processes:** Work can be done manually while IT systems are down.
- **Outsourcing:** Some work can be performed by external companies, competitors (reciprocal agreement), or secondary vendors.
- **Disaster recovery for IT:** An IT recovery solution will be needed for critical systems, but because these can be very expensive, manual work processes may be used initially following a disaster.
- **Alternative staffing:** Identify other staff members who can perform the job function.
- **Alternative facilities:** Identify alternative facilities where the primary staff can work.

RTO vs. RPO


GTAG-10_Biz-Cont_forWeb-CX1_BCP.pdf - Adobe Acrobat
File Edit View Window Help
Create
10
(14 of 40)
200%
Tools
Comment
10
8.50 x 11.00 in
11:07 AM
4/4/2013

erformed by the functional team, the resources needed to erform the function, and the critical staff performing the vork. The business processes initially should not be broken lown into too many individual sub-processes. Business rocesses should be identified separately if they have different taffing (e.g., staff roles), service providers (e.g., third party, utsourcer, etc.), or resources (e.g., IT systems).

exchange data with the organization system (e.g systems). The business management ultimately the correct RPO for each business process. Typ cost of the recovery solution will rise as the RPO (i.e., if the business process cannot afford to lose any data, the cost of data replication could be very expensive).

Processing Gap: Lag time between the disruption point and resumption of normal processing.

This represents the data that will be lost, destroyed, or otherwise unavailable, after successful recovery.

igure 4. Understanding RTO and RPO

Storage – RAID (CISA Review Manual)

Level	Techniques	Description	Pros/Cons
RAID-0	Disk striping	Data is distributed on stripes that are sent to each disk in the array.	Best performance but No fault tolerance
RAID -1	Disk mirroring	Data on one disk is mirrored on another.	100% redundancy of data slow performance and 50% loss of storage space
RAID -5	Striping with parity	Data and parity are striped in blocks across all disks	High Read data transaction rate; redundancy; Complex controller design
RAID - 10	Disk striping AND mirroring	Striped array’s segments are mirrored.	Redundancy + High performance; expensive

Risk Monitoring and Testing

- **Objectives:**
  - Incorporation of the BIA and risk assessment into the BCP and testing program;
  - Development of an enterprise-wide testing program;
  - Assignment of roles and responsibilities for implementation of the testing Business Continuity Planning program;
  - Completion of annual, or more frequent, tests of the BCP;
  - Evaluation of the testing program and the test results by senior management and the board;
  - Assessment of the testing program and test results by an independent party; and
  - Revision of the BCP and testing program based upon changes in business operations, audit and examination recommendations, and test results.

Risk Monitoring and Testing (cont.)

Testing Principles

- Roles and responsibilities for implementation and evaluation of the testing program should be specifically defined;
- The BIA and risk assessment should serve as the foundation of the testing program, as well as the BCP that it validates;
- The breadth and depth of testing activities should be commensurate with the importance of the business process to the institution, as well as to critical financial markets;
- Enterprise-wide testing should be conducted at least annually, or more frequently, depending on changes in the operating environment;

Risk Monitoring and Testing (cont.)

Testing Principles

- Testing should be viewed as a continuously evolving cycle, and institutions should work towards a more comprehensive and integrated program that incorporates the testing of various interdependencies;
- Institutions should demonstrate, through testing, that their business continuity arrangements have the ability to sustain the business until permanent operations are reestablished;
- The testing program should be reviewed by an independent party; and
- Test results should be compared against the BCP to identify any gaps between the testing program and business continuity guidelines, with notable revisions incorporated into the testing program or the BCP, as deemed necessary.

Risk Monitoring and Testing (cont.)

Testing Strategies

- Expectations for business lines and support functions to demonstrate the achievement of business continuity test objectives consistent with the BIA and risk assessment;
- A description of the depth and breadth of testing to be accomplished;
- The involvement of staff, technology, and facilities;
- Expectations for testing internal and external interdependencies; and
- An evaluation of the reasonableness of assumptions used in developing the testing strategy.

Risk Monitoring and Testing (cont.)

Testing Scope and Objectives

- Not jeopardize normal business operations;
- Gradually increase the complexity, level of participation, functions, and physical locations involved;
- Demonstrate a variety of management and response proficiencies under simulated crisis conditions, progressively involving more resources and participants;
- Uncover inadequacies so that testing procedures can be revised;
- Consider deviating from the test script to interject unplanned events, such as the loss of key individuals or services; and
- Involve a sufficient volume of all types of transactions to ensure adequate capacity and functionality of the recovery facility.

Risk Monitoring and Testing (cont.)

Testing Plan

- A master test schedule that encompasses all test objectives;
- Specific description of test objectives and methods;
- Roles and responsibilities for all test participants, including support staff;
- Designation of test participants;
- Test decision makers and succession plans;
- Test locations; and
- Test escalation conditions and test contact information.

Risk Monitoring and Testing (cont.)

Testing Methods

- Desk Check or Plan Audit
- Orientation or Plan Walkthrough
- Tabletop Exercise (Boardroom style exercise)
- Communication Testing
- IT Environment (Systems and Application) Walkthrough
- Alternative Site Testing
- End-to-end Testing
- **Execution, Evaluation, Independent Assessment, and Reporting of Test Results**

Other Related Policies, Standards and Procedures

- Security Standards;
- Project Management;
- Change Control Policies;
- Data Synchronization Procedures;
- Crises Management;
- **Incident Response;**
- Remote Access;
- Employee Training;
- Notification Standards;
- Insurance; and
- Government and Community.

Pandemic Planning

- Definition: *“Pandemics are defined as epidemics or outbreaks in humans of infectious diseases that have the ability to spread rapidly over large areas, possibly worldwide. Several pandemics have occurred throughout history, and experts predict that we will experience at least one pandemic outbreak in this century. “*

Pandemic Planning

- A preventive program
- A documented strategy
- Comprehensive framework of facilities, systems, or procedures
- A testing program
- An oversight program to ensure ongoing review and updates

Pandemic Planning (cont.)

- Resources:

  http://www.pandemicflu.gov/ (DHHS)

  https://www.fsscc.org/influenza/financial panning.jsp

  http://www.pandemicflu.gov/plan/pdf/cikrpandemicinfluenzaguide.pdf (DHS)

  http://www.pandemicflu.gov/plan/community/commitigation.html (CDC)

IT – Disaster Recovery

- *“Disaster recovery of information technology (IT) components supports restoring operations critical to the resumption of business, including regaining access to data (records, hardware, software, etc.), communications (e-mail, phone, etc.), workspace, and other business processes after a disaster. A well-established and thoroughly tested disaster recovery plan must be developed in harmony with the BCM plan to increase the probability of successfully recovering vital organization records.” – GTAG Business Continuity Management*

IT – Disaster Recovery

- *Recovery of Critical IT Components*
  - IT systems, including:
    - IT data center.
      - Applications and data needed by the organization.
      - Servers and other hardware.
      - Communications such as phone, radio, etc.
      - Network, including external (third party) connections.
      - IT infrastructure (e.g., logon services and software distribution).
      - Remote access services.
      - Process control systems (e.g., SCADA/DCS).
    - Information management systems, including:
      - File rooms.
      - Document management systems (electric and manual).

Recovery Solutions and Sites

- Hot recovery plan/capabilities.
  - A recovery plan exists.
  - Recovery resources are available at recovery site(s) and data is synchronized in real-time to enable the system to be recovered immediately or within hours.
  - Typical recovery time is minutes to one day.
- Warm recovery plan/capabilities.
  - A recovery plan exists.
  - Recovery resources (e.g., nonproduction systems, spare hardware, etc.) are available at recovery site(s) but may need to be configured to support the production system when the disaster occurs.
  - Some data may need to be restored (probably from tape or other backups).
  - Typical recovery time is two to 13 days.

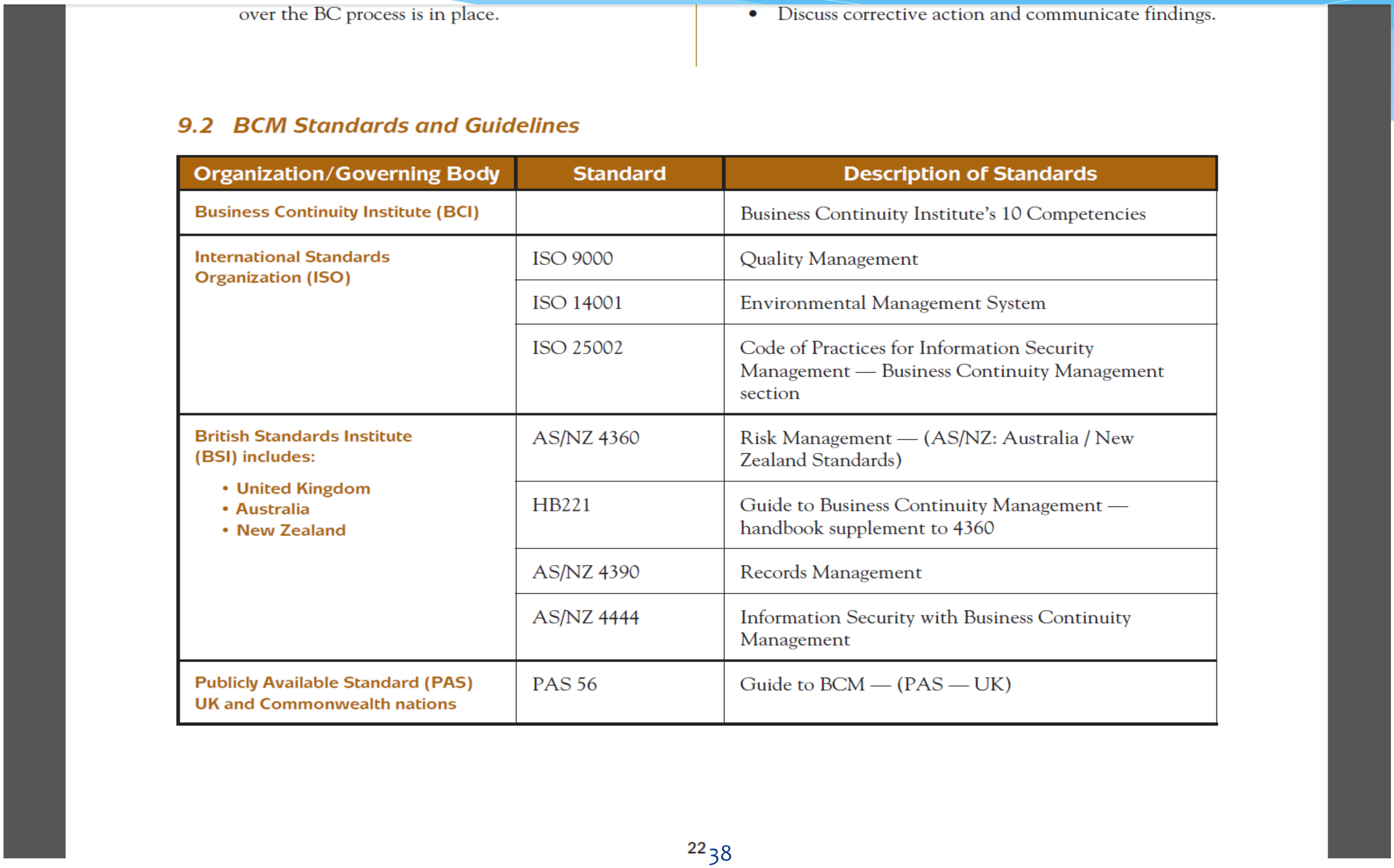
Recovery Solutions and Sites

- Cold recovery plan/capabilities.
  - A recovery plan exists.
  - Recovery site(s) have been identified with space and base infrastructure needed to perform the recovery.
  - Recovery resources (e.g., servers) are not available at recovery site(s) and likely need to be procured.
  - Data likely needs to be restored (probably from tape backups).
  - Typical recovery time is 14 to 30 days.
- No recovery plan/capabilities.
  - No recovery plan exists.
  - Recovery resources and data restore processes have not been defined.
  - Data backup plans exist to ensure that critical data can be restored at some time in the future.
  - A risk exists that the systems and business processes they support may never be recovered or may result in an extended delayed recovery.

BCP Audit Program

- Determine examination scope and objectives for reviewing the business continuity planning program.
- Determine the quality of business continuity plan oversight and support provided by the board and senior management.
- Determine whether an adequate BIA and risk assessment have been completed.
- Determine whether appropriate risk management over the business continuity process is in place.
- Determine the existence of an appropriate enterprise-wide BCP.
- Determine whether the BCP includes appropriate hardware back-up and recovery.
- Determine that the BCP includes appropriate security procedures
- Determine whether the BCP effectively addresses pandemic issues.
- Determine whether the BCP addresses critical outsourced activities.
- Determine whether the BCP testing program is sufficient to demonstrate the financial institution's ability to meet its continuity objectives.
- Discuss corrective action and communicate findings.

Standards and Guidlines



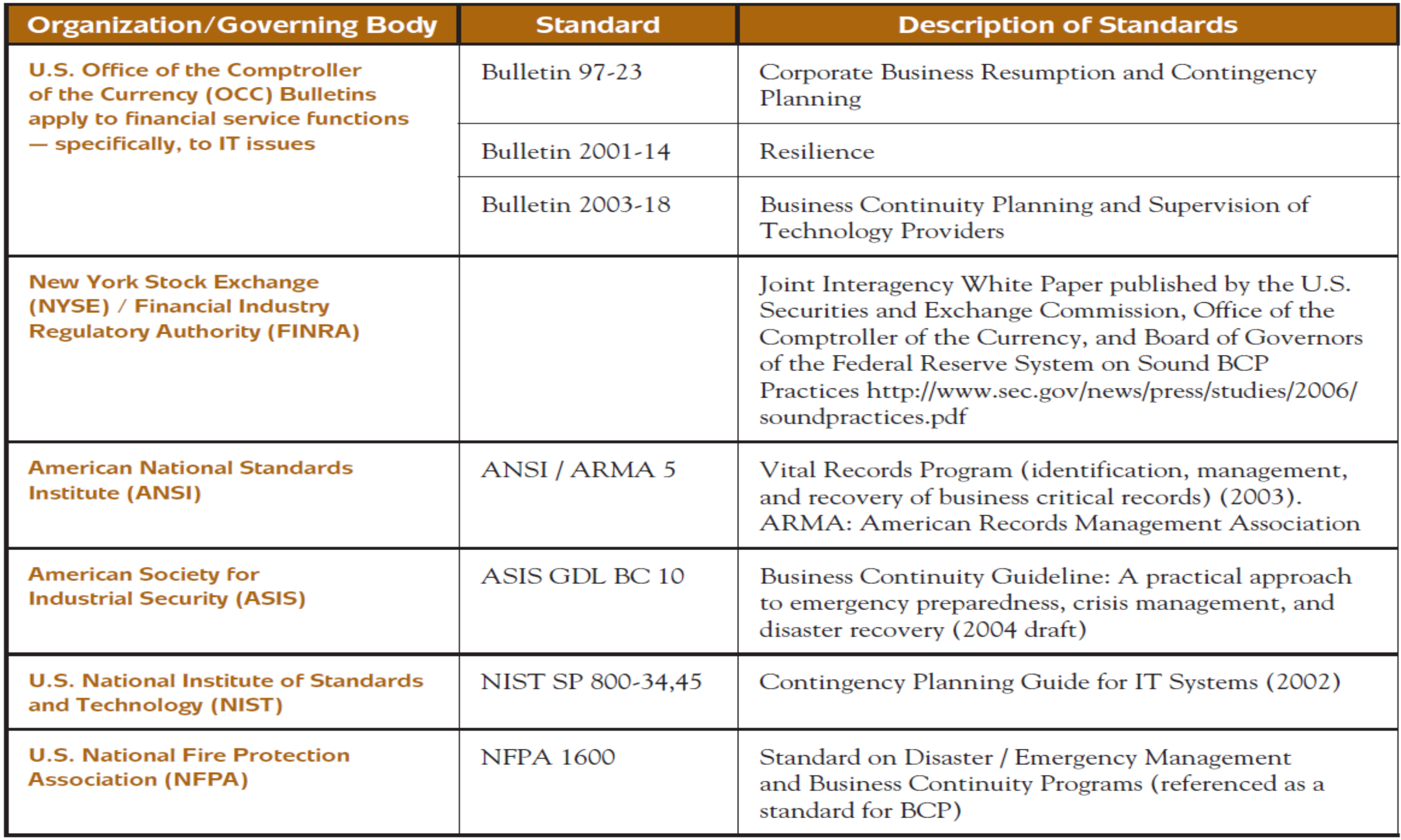
over the BC process is in place.

- Discuss corrective action and communicate findings.

9.2 BCM Standards and Guidelines

Organization/Governing Body	Standard	Description of Standards
Business Continuity Institute (BCI)		Business Continuity Institute's 10 Competencies
International Standards Organization (ISO)	ISO 9000	Quality Management
	ISO 14001	Environmental Management System
	ISO 25002	Code of Practices for Information Security Management — Business Continuity Management section
British Standards Institute (BSI) includes: • **United Kingdom** • **Australia** • **New Zealand**	AS/NZ 4360	Risk Management — (AS/NZ: Australia / New Zealand Standards)
	HB221	Guide to Business Continuity Management — handbook supplement to 4360
	AS/NZ 4390	Records Management
	AS/NZ 4444	Information Security with Business Continuity Management
Publicly Available Standard (PAS) UK and Commonwealth nations	PAS 56	Guide to BCM — (PAS — UK)

Standards and Guidelines



Organization/Governing Body	Standard	Description of Standards
U.S. Office of the Comptroller of the Currency (OCC) Bulletins apply to financial service functions — specifically, to IT issues	Bulletin 97-23	Corporate Business Resumption and Contingency Planning
	Bulletin 2001-14	Resilience
	Bulletin 2003-18	Business Continuity Planning and Supervision of Technology Providers
New York Stock Exchange (NYSE) / Financial Industry Regulatory Authority (FINRA)		Joint Interagency White Paper published by the U.S. Securities and Exchange Commission, Office of the Comptroller of the Currency, and Board of Governors of the Federal Reserve System on Sound BCP Practices http://www.sec.gov/news/press/studies/2006/soundpractices.pdf
American National Standards Institute (ANSI)	ANSI / ARMA 5	Vital Records Program (identification, management, and recovery of business critical records) (2003). ARMA: American Records Management Association
American Society for Industrial Security (ASIS)	ASIS GDL BC 10	Business Continuity Guideline: A practical approach to emergency preparedness, crisis management, and disaster recovery (2004 draft)
U.S. National Institute of Standards and Technology (NIST)	NIST SP 800-34,45	Contingency Planning Guide for IT Systems (2002)
U.S. National Fire Protection Association (NFPA)	NFPA 1600	Standard on Disaster / Emergency Management and Business Continuity Programs (referenced as a standard for BCP)