AUDITING A BCP PLAN

What are the Objectives of a Good BCP Plan

- Protect employees
- Restore critical business processes or functions to minimize the financial impact of a disaster
- Restore related infrastructure, operating systems and applications to support the critical functions
- Prevent or mitigate the effects of a disaster from occurring wherever possible
- Protect corporate assets
- Minimize legal exposure

Where to Start

Obtain the following documentation

- Organizational Charts and Business Process Analysis
- Overall Recovery Plan Structure
- Plan Coordinator List
- Business Impact Analysis
- Risk Assessment
- Recovery Plan Documentation
- Third Party Review (of available)

Audit Steps – Business Process Analysis

- Was a high level business process analysis performed?
- Has the Plan Unit organization structure been identified and documented?
- Is the organization and location structure current, change management?
- Have business impact criteria been defined?

Audit Steps – Business Impact Analysis (BIA)

- Was a BIA performed and documented in alignment with the criteria established?
- Was there an established methodology used to perform the BIA and document the results of the analysis?
- Is there adequate documentation for assumptions and impact scoring rationale?
- Were the final BIA results approved by senior management?
- Do recovery strategies align with the results of the BIA?
- Have Recovery Time Objectives and Recovery Point Objectives been identified?

Audit Steps – Risk Assessment and Mitigation – Life Safety

- Has an emergency Coordinator been appointed?
- Has a review been conducted to determine potential risks of natural disasters and other building emergencies?
- Have mitigation strategies been identified and implemented?

Risk Assessment and Mitigation Facility/Technology/Business Operations

- Was a facility, Technology and Business Operations Risk Assessment conducted that:
  - Identifies control weaknesses and single points of failure
  - Identifies one or more countermeasures

- Have mitigation strategies been selected and implemented?

Audit Steps – Risk Assessment and Mitigation – Third Parties

- Have all critical third parties been identified and linked to the business process and related infrastructure / technology identified in the BIA?
- Have third party review criteria been established?
- Was a third party risk assessment performed by vendor?

Audit Steps – Recovery Plans

- Are Recovery roles identified?
- Has an individual and a backup been identifed who can declare a disaster?
- Is the plan documentation current and has it been distributed to all personnel?
- Are Emergency Notification Procedures clear and accurate?
- Are Communication procedures in place and current (who talks to who)?
- Are recovery requirements and data current?

Audit Steps – Exercise, Maintenance and Training

- Has an Exercise, Maintenance, and training program been developed, implemented and communicated that includes?
  - Key elements to be maintained
  - Key Elements to be exercised
  - An Exercise and maintenance calendar
  - Specific exercises conducted
  - Recommendations and follow-up for improvement

Audit Steps – Change Control

- Are there change control procedures?
- Are changes formally approved before implementation?
- Is there document version control procedures established?
- Are there procedures for incorporating changes and notification?

Confidentiality and Integrity of an Audit

The confidentiality, integrity and availability of information systems must be ensured to protect the business from the risks relating to information technology.

An IS audit helps to identify areas where these are vulnerable or inadequately protected through systematic examination and evaluation.

The dependence of today’s enterprises on IT is significant. For an organization that uses IT extensively for its operations, not just recording of transactions, the non-availability of its information systems could mean the end of its existence.

Availability of Audit Results

Availability is one of the major criteria for IS audit.

Availability is ensured through various means, technologies and processes -- all broadly covered under the umbrella of business continuity and disaster recovery.

Why BCP Audits are needed

An IS audit of business continuity is essentially an audit of this plan with reference to:

- The adequacy, completeness and appropriateness of the plan;
- Availability of the processes and people to implement the plan;
- Its testing; and
- The verification of the various day-to-day functions that need to be performed to make the plan effective and ready at all times.

BCP Audit Basic Steps

The audit of business continuity can be broken into three major components:

1. Validating the business continuity plan
2. Scrutinizing and verifying preventive maintenance and facilitating measures for ensuring continuity
3. Examining evidence about the performance of activities that can assure continuity and recovery

BCP Audits Validate the BC Plan

Validating the Business Continuity Plan

The IS auditor should be familiar with the business, the information systems in use and the extent of the business' dependence on IT. The auditor's focus should be on validating the plan against this knowledge.

The following points are written with this objective and are not meant to be a comprehensive description of everything that should be in the business continuity plan:

BCP Audit Scope

- The IS auditor should check whether the plan covers all mission-critical systems or is only for other, selected systems.
- The IS auditor should ascertain whether the plan is based on a systematic business impact analysis that clearly understands the impact of non-availability of the systems on the business
- The auditor should examine the plan to determine whether the plan has a good combination of preventive controls and recovery controls.
- The IS auditor should also verify whether the BCP is updated periodically and reflects the current business and IT environment accurately.

BCP Audit Aspects

- Another important aspect to be evaluated in the BCP is the requirement of testing the plans or disaster recovery drills.
- The BCPs other elements, like notifications, call trees, the response teams, updating the contact information, and the step-by-step procedures for recovery, should be evaluated for appropriateness from the IS auditor's knowledge of the business.
- The auditor should verify whether the plan addresses not just recovery after a disaster but also restoration back to the primary site when normalcy returns.

Scrutinizing and Verifying Preventive Maintenance and Facilitating Measures for Ensuring Continuity

The verification of the physical facilities and the equipment and environment that ensure availability and recovery after a disaster includes the following:

- The IS auditor should verify the existence and correct functioning of all the preventive controls.
- The scrutiny of the disaster recovery site as to its location (i.e., distance from primary site, accessibility, vulnerability to similar threats) and the general controls and security relating to it should be an essential part of the audit.

BCP Audit of DR Site

- The DR site and the tape storage site could be different locations, in which case the auditor should also verify the offsite storage facility with respect to the preventive controls, such as physical security, fire and flood controls, etc.

The IS auditor should verify the contracts entered into by the SLAs and whether the periodic testing and drills are being performed as agreed.

The IS auditor should verify that supporting equipment and supplies, such as fuel for the power generators, are maintained to enable usage of the redundant equipment when required.

BCP Audit DR Site Facilities

The auditor should verify whether there are facilities for alternate routes to overcome network failures. The auditor also needs to check the availability of the network at the DR site and the facilities for switchover from the primary site during recovery to enable all users to access the systems from the DR site.

Examining Evidence About the Performance of Activities That Can Assure Continuity and Recovery

Effective recovery is not completed by merely acting on the day of the disaster, but by sustained activities that are completed in due course with the objective of remaining in a state of preparedness for a disaster. A number of activities need to be performed on a day-to-day basis to ensure availability of systems at all times, as required, and recovery following a disaster.

BCP Audit of Vital Records

The IS auditor should verify the backup tapes with respect to the backup logs and the labeling of the tapes and other records to check whether the backups are being taken as prescribed in the plan at the required intervals.

Verification of maintenance and testing logs of all equipment, such as power generators, air conditioners, UPS systems and fire control equipment, can give the IS auditor clues as to the effectiveness of these controls.

The most important part of the verification is to see whether the plan has been tested and, if so, how thoroughly tested.

BCP Audit of People and their Functional Responsibilities

The IS auditor should not ignore the people part of the BCP. Training programs and awareness campaigns are essential, especially in large organizations, to ensure that the plans actually work on the day when disaster strikes.

Conclusion

The nature, complexity and cost of the business continuity program are related to the nature of the business' dependence on information technology.

While the testing of business continuity plans with various testing techniques and drills is the best possible way to ensure that the plans and the expensive systems deployed really work on the day of disaster, such tests have some limitations as they often need to be planned in advance. An effective audit review by a capable IS auditor can help uncover many deficiencies and operational lapses that may not come up in testing and points that have been overlooked in the design of the plan.