Business Continuity Planning for Risk Reduction

Ion PLUMB
ionplumb@yahoo.com
Andreea ZAMFIR
zamfir_andreea_ileana@yahoo.com
Delia TUDOR
tudordelia@yahoo.com
Faculty of Management
Academy of Economic Studies Bucharest

Abstract. The paper outlines the business continuity planning as a methodology that could be used by organizations in order to reduce the risks that occur both at the organizational level and in its outside environment. There are presented the main objectives and steps in business continuity planning process. In the end of the paper are presented some issues that organizations should take into consideration in the implementation of business continuity planning process projects.

Keywords: business continuity planning, business impact analysis, risk assessment, risk management, risk monitoring.

1. Introduction

Business continuity planning (BCP) is an interdisciplinary peer mentoring methodology used to create and validate a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical function(s) within a predetermined time after a disaster or extended disruption. Business continuity planning means actually how an organization prepares for future incidents that could jeopardize the organization's core mission and its long term health. Incidents include local incidents like building fires, regional incidents like earthquakes, or national incidents like pandemic illnesses. Business continuity planning may be, for example, part of the organizational learning effort that helps reducing operational risk associated with lax information management controls. This process may be integrated with improving information security and corporate reputation risk management practices. An organization’s business continuity planning process should take into consideration the following objectives: business continuity planning is about maintaining, resuming and recovering the business; 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 business continuity planning; the effectiveness of a business continuity planning can be validated only through testing or practical application; the business continuity planning and test results should be subjected to an independent audit; a business continuity planning should be periodically updated to reflect and respond to changes that occur both at the organizational level and in its outside environment.

2. Steps in the business continuity planning process

The organizations could adopt a process-oriented approach to business continuity planning and this process should involve: business impact analysis, risk assessment, risk management, risk monitoring. The business continuity planning lifecycle can be represented as shown in figure no 1.

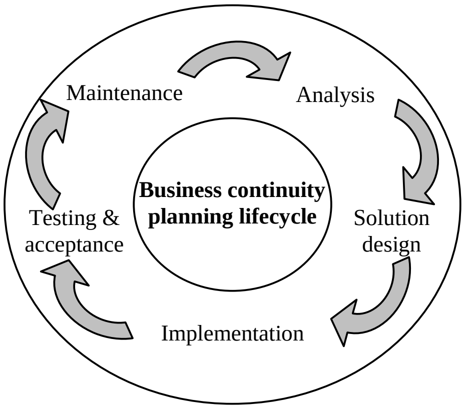

Figure 1. Business continuity planning lifecycle

2.1. Business impact analysis

The first step in the business continuity planning process, the business impact analysis, should include: identification of the potential impact of uncontrolled, non-specific events on the institution’s business process and its customers; consideration of all departments and business functions.

The business impact analysis phase identifies the potential impact of uncontrolled, non-specific events on the institution's business processes. The business impact analysis phase also should determine what and how much is at risk by identifying critical business functions and prioritizing them. It should estimate the maximum allowable downtime for critical business processes, recovery point objectives and backlogged transactions, and the costs associated with downtime.

Management should establish recovery priorities for business processes that identify essential personnel, technologies, facilities, communications systems, vital records, and data. The business impact analysis also considers the impact of legal and regulatory requirements such as the privacy and availability of customer data and required notifications to the institution's primary federal regulator and customers when facilities are relocated.

Personnel responsible for this phase should consider developing uniform interview and inventory questions that can be used on an enterprise-wide basis. Uniformity can improve the consistency of responses and help personnel involved in the business impact analysis phase compare and evaluate business process requirements. This phase may initially prioritize business processes based on their importance to the institution's achievement of strategic goals and maintenance of safe and sound practices. However, this prioritization should be revisited once the business processes are modeled against various threat scenarios so that a business continuity planning can be developed. The amount of time and resources necessary to complete the business impact analysis will depend on the size and complexity of the financial institution.

2.2. Risk assessment

The risk assessment step is critical and has significant bearing on whether business continuity planning efforts will be successful. If the threat scenarios developed are unreasonably limited, the resulting may be inadequate. During the risk assessment step, business processes and the business impact analysis assumptions are stress tested with various threat scenarios. This will result in a range of outcomes, some that require no action for business processes to be successful and others that will require significant business continuity planning to be developed and supported with resources (financial and personnel).

Organizations should develop realistic threat scenarios that may potentially disrupt their business processes and ability to meet their client's expectations (internal, business partners, or customers). Threats can take many forms, including malicious activity as well as natural and technical disasters. Where possible, institutions should analyze a threat by focusing on its impact on the institution, not the nature of the threat. For example, the effects of certain threat scenarios can be reduced to business disruptions that affect only specific work areas, systems, facilities (i.e., buildings), or geographic areas.

Additionally, the magnitude of the business disruption should consider a wide variety of threat scenarios based upon practical experiences and potential circumstances and events. If the threat scenarios are not comprehensive, business continuity planning may be too basic and omit reasonable steps that could improve business processes' resiliency to disruptions. Threat scenarios need to consider the impact of a disruption and probability of the threat occurring.

Threats could have a high probability of occurrence and low impact to the institution (e.g., brief power interruptions), or a low probability of occurrence and high impact on the institution (e.g., hurricane, terrorism). High probability threats are often supported by very specific business continuity planning. However, the most difficult threats to address are those that have a high impact on the institution but a low probability of occurrence. Using a risk assessment, business continuity planning may be more flexible and adaptable to specific types of disruptions that may not be initially considered.

It is at this point in the business continuity planning process that organizations should perform a "gap analysis." In this context, a gap analysis is a methodical comparison of what types of plans the institution (or business line) needs to maintain, resume, or recover normal business operations in the event of a disruption, versus what the existing business continuity planning provides. The difference between the two highlights additional risk exposure that management and the board need to address in business continuity planning development.

The risk assessment considers: the impact of various business disruption scenarios on both the institution and its customers; the probability of occurrence based, for example, on a rating system of high, medium, and low; the loss impact on information services, technology, personnel, facilities, and service providers from both internal and external sources; the safety of critical processing documents and vital records; a broad range of possible business disruptions, including natural, technical, and human threats.

When assessing the probability of a specific event occurring, organizations and technology service providers should consider the geographic location of facilities and their susceptibility to natural threats (e.g., location in a flood plain), and the proximity to critical infrastructures (e.g., power sources, nuclear power plants, airports, points of interest, major highways, railroads). The risk assessment should include all the organizations or service provider's locations and facilities. Worst-case scenarios, such as destruction of the facilities and loss of life, should be considered. At the conclusion of this phase, the institution will have prioritized business processes and estimated how they may be disrupted under various threat scenarios.

2.3. Risk management

After conducting the business impact analysis and risk assessment, management should prepare a written business continuity planning. The plan should document strategies and procedures to maintain, resume, and recover critical business functions and processes and should include procedures to execute the plan's priorities for critical vs. non-critical functions, services and processes. A well-written business continuity planning should describe in some detail the types of events that would lead up to the formal declaration of a disruption and the process for invoking the business continuity planning. It should describe the responsibilities and procedures to be followed by each continuity team and contain contact lists of critical personnel. The business continuity planning should describe in detail the procedures to be followed to recover each business function affected by the disruption and should be written in such a way that various groups of personnel can implement it in a timely manner.

A business continuity planning is more than recovery of the technology, but rather a recovery of all critical business operations. The plan should be flexible to respond to changing internal and external conditions and new threat scenarios. Rather than being developed around specific events (e.g. fire vs. tornado), the plan will be more effective if it is written to adequately address specific types of scenarios and the desired outcomes. A business continuity planning should describe the immediate steps to be taken during an event in order to minimize the damage from a disruption, as well as the action necessary to recover. Thus, business continuity planning should be focused on maintaining, resuming, and recovering the institution's operations after a disruption. Specific scenarios should include how the financial institution would respond if:

- Critical personnel is not available;
- Critical buildings, facilities, or geographic regions are not accessible;
- Equipment malfunctions (hardware, telecommunications, operational equipment);
- Software and data are not accessible or are corrupted;
- Vendor assistance or service provider is not available;
- Utilities are not available (power, telecommunications);
- Critical documentation and/or records are not available.

Organizations should carefully consider the assumptions on which the business continuity planning is based. Also, institutions should not assume a disaster will be limited to a single facility or a small geographic area. Institutions should not assume they will be able to gain access to facilities that have not been damaged or that critical personnel (including senior management) will be available immediately after the disruption. Assuming public transportation systems such as airlines, railroads and subways will be operating may also be incorrect. Organizations should not assume the telecommunications system will be operating at normal capacity.

A business continuity planning consists of many components that are both internal and external to a financial institution. The activation of a continuity plan and restoration of business in the event of an emergency is dependent on the successful interaction of various components. The overall strength and effectiveness of a business continuity planning can be decreased by its weakest component.

An effective business continuity plan coordinates across its many components, identifies potential process or system dependencies, and mitigates the risks from interdependencies.
Typically, the business continuity coordinator or team facilitates the identification of risk and the development of risk mitigation strategies across business areas. Internal causes of interdependencies can include line of business dependencies, telecommunication links, and/or shared resources (i.e., print operations or e-mail systems). External sources of interdependencies that can negatively impact a business continuity plan can include telecommunication providers, service providers, customers, business partners and suppliers.

2.4. Risk monitoring

Risk monitoring is the final step in business continuity planning. It should ensure that the institution's business continuity planning is viable through:

- Testing the business continuity planning at least annually;

- Subjecting the business continuity planning to independent audit and review;
- Updating the business continuity planning based upon changes to personnel and the internal and external environments.

3. Implementation of business continuity planning projects

Organizations should provide business continuity training for personnel to ensure all parties are aware of their responsibilities should a disaster occur. Key employees should be involved in the business continuity development process, as well as periodic training exercises. The training program should incorporate enterprise-wide training as well as specific training for individual business units. Employees should be aware of which conditions call for implementing all or parts of the business continuity planning, who is responsible for implementing business continuity planning for business units and the institution, and what to do if these key employees are not available at the time of a disaster. Cross training should be utilized to should be regularly scheduled and updated to address changes to the business continuity planning.

Communication planning should identify alternate communication channels to use during a disaster, such as pagers, cell phones, e-mail, or two-way radios. An emergency telephone number, e-mail address, and physical address list should be provided to employees to assist in communication efforts during a disaster. The list should provide all alternate numbers since one or more telecommunications systems could be unavailable. Additionally, the phone list should provide numbers for vendors, emergency services, transportation, and regulatory agencies. Wallet cards, Internet postings, and calling trees are possible ways to distribute information to employees. Further, institutions should establish reporting or calling locations to assist them in accounting for all personnel following a disaster. Organizations should consider developing an awareness program to let customers, service providers, and regulators know how to contact the institution if normal communication channels are not in operation. The plan should also designate personnel who will communicate with the media, government, vendors, and other companies and provide for the type of information to be communicated.

In order to recoup losses from risks that cannot be completely prevented organizations are often using insurance. Generally, insurance coverage is obtained for risks that cannot be entirely controlled, yet could represent a significant potential for financial loss or other disastrous consequences. The decision to obtain insurance should be based on the probability and degree of loss identified during the business impact analysis. Organizations should determine potential exposure for various types of disasters and review the insurance options available to ensure appropriate insurance coverage is provided. Management should know the limits and coverage detailed in insurance policies to make sure coverage is appropriate given the risk profile of the institution. Institutions should perform an annual insurance review to ensure the level and types of coverage are commercially reasonable, and consistent with any legal, management, and board requirements. Also, institutions should create and retain a comprehensive hardware and software inventory list in a secure off-site location in order to facilitate the claims process. Organizations should be aware of the limitations of insurance. Insurance can reimburse an institution for some or all of the financial losses incurred as the result of a disaster or other significant event. However, insurance is by no means a substitute for an effective business continuity planning, since its primary objective is not the recovery of the business. For example, insurance cannot reimburse an institution for damage to its reputation.

An institution may need to coordinate with community and government officials and the news media to ensure the successful implementation of the business continuity planning. Ideally, these relationships should be established during the planning or testing phases of business continuity planning. This establishes proper protocol in case a city-wide or region-wide event impacts the institution's operations. Organizations are encouraged to contact state and local authorities during the risk assessment process to inquire about specific risks or exposures for all their geographic locations and special requirements for accessing emergency zones. During the recovery phase, facilities access, power, and telecommunications systems would be coordinated with various entities to ensure timely resumption of operations.

Conclusions

A business continuity planning is a "living" document; changing in concert with changes in the business activities it supports. The plan should be reviewed by senior management, the planning team or coordinator, team members, internal audit, and the board of directors at least annually. As part of that review process, the team, or coordinator should contact business unit managers throughout the financial institution at regular intervals to assess the nature and scope of any changes to the institution's business, structure, systems, software, hardware, personnel, or facilities. It is to be expected that some changes will have occurred since the last plan update. Software applications are commercially available to assist the business continuity planning coordinator in identifying and tracking these organizational changes so that the business continuity planning can be updated.

All such organizational changes should be analyzed to determine how they may affect the existing continuity plan, and what revisions to the plan may be necessary to accommodate these changes. The agencies expect that business continuity planning updates will be documented to show that the plan reflects the institution, as it currently exists. Lastly, the financial institution should ensure the revised business continuity planning is distributed throughout the organization.

References

1. *Barnes, James, A Guide to Business Continuity Planning, John Willey and Sons Ltd, UK, 2001.*
2. *Barnes, Peter, Hiles, Andrew, The Definitive Handbook of Business Continuity Management, John Willey and Sons Ltd, UK, 2001.*
3. *Toigo, William, Disaster Recovery Planning, Prentice Hall, 2003.*