A project planning process for business continuity

Kon Karakasidis
KPMG Information Technology Consulting Division, Melbourne, Australia

Discusses the formulation of a business recovery plan. As a starting point, presents the business recovery timeline model. Gives a framework of components to be considered in a business continuity project planning process, i.e. a risk reduction programme.

This article first appeared in *Information Management & Computer Security*, Vol. 5 No. 2, 1997, pp. 72-78.

Industrial Management & Data Systems
97/8 [1997] 320–326

[ISSN 0263-5577]

In the last few years, disaster recovery (DR) practitioners (for IT systems) and business recovery (BR) practitioners (for core business activities) have both agreed that recovering IT systems and services will not ensure the survival of the business.

As a result of "real-life lessons learned" from disaster situations, recovery practitioners are constantly inundated with a vast array of contingency methodologies, tools, templates, consulting services, etc. Auditors are also finding themselves in constant "refinement mode" as they review their audit processes and methodologies to ensure the right questions are asked when conducting reviews of BR/DR plans, frameworks, strategies, guidelines, policies and standards. A never ending story – or is it?

Based on such "never ending" real-life experiences, one crucial element has surfaced: "consider all risks when building a business recovery plan and if you think your disaster scenario based plan will save your business if a problem escalates for whatever unforeseen reason, you are in for a big shock!" Arnott's recent product tampering (poisoning of biscuit products) in Australia is just one case. Would your business continuity process handle product tampering?

Disaster scenario based plans are basically plans built around a specific disaster. Just ask those who have "been there, done that"; they will tell you that comprehensiveness and flexibility must be built into the business continuity process. Figure 1 is an excellent starting point: it clearly shows the path taken in the event of a problem escalating to a disaster, or of some event that necessitates the declaration of a disaster.

A requirement of the business continuity planning process is to instigate a "risk reduction programme". This will ensure that company threats (refer to Tables I and II) are identified and assessed accordingly.

After having identified the risks, "managing" them within the business recovery timeline should be a straightforward process. The end result being a "business continuity – the total solution" process.

A business continuity project planning process comprises the following components and should be used in conjunction with a broad risk management process, i.e. risk reduction programme:

1 Obtain top management approval and support.
2 Establish a business continuity planning (BCP) committee.
3 Perform business impact analyses.
4 Evaluate critical needs and prioritize business requirements.
5 Determine the business continuity strategy and associated recovery process.
6 Prepare business continuity strategy and its implementation plan for executive management approval.
7 Prepare business recovery plan templates and utilities, finalize data collection and organize/develop the business recovery procedures.
8 Develop the testing criteria and procedures.
9 Test the business recovery process and evaluate test results.
10 Develop/review service level agreement(s) (SLAs).
11 Update/revise the business recovery procedures and templates.

The following sections describe and discuss each of the above components.

Obtain top management approval and support

A prolonged disruption, crisis or disaster could result in loss of vital corporate assets, market share and/or business momentum. To protect the organization, a comprehensive business continuity process and detailed plan must be accepted as an insurance policy.

The successful implementation of a business continuity process requires an effort, particularly by executive management, to recognize the disruptive impact of intentional and unintentional threats as a business problem.

To develop an effective business continuity process, it is imperative that executive management thoroughly understand, approve and authorize all resulting and supporting activities. They must be willing to commit the required labour and funds necessary for

Figure 1
Business recovery timeline

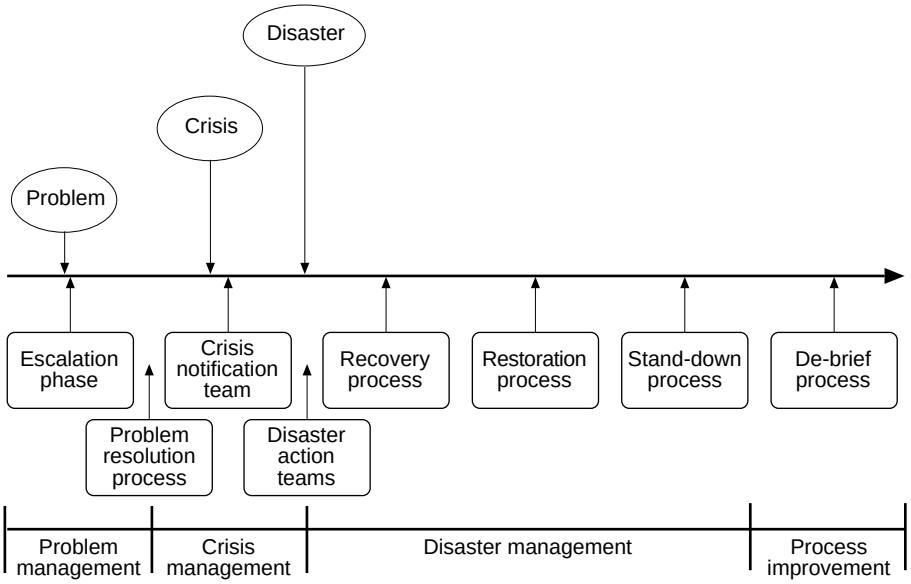

Table I
Intentional threats

Cause	Effect
Arson	Any fire related damage – refer fire
Bomb threats	Building evacuation, time to search/detect, diffuse and/or declare safe, return to normal
Civil disturbances	Building occupancy, denial of access to staff, suppliers, customers, etc. possible minor injury to staff, interruption to rosters, etc.
Criminal acts	Damage of equipment and/or communications. Can be non-IT and IT related, whether internally/externally originated/executed
Data disclosure or corruption	Deliberate theft and disclosure, whether for profit or not, deliberate program code manipulation, coded time bombs – trojan horses/viruses
Data entry errors	Errors of commission and omission as both intentional (unproven) and unintentional
Extortion	Hostage taking, ransom demands, etc. for data, staff, customers, etc. whether originating from single criminal actions, activists, saboteurs, terrorists, etc.
Hacking	Refer data disclosure or corruption
Hostage taking	Refer extortion
Industrial action	*Within the organizational sphere*: including strikes, lockouts; go-slow actions, work to regulations, non-handling/processing, etc. *External*: transport, telecommunication, utility services supply, etc.
Riot	Refer civil disturbances
Vandalism	May directly or indirectly cause fuss of either processing ability to customers, or organizational services (internal/external)

business continuity process and plan(s) development, implementation, testing and subsequent maintenance.

Establish a business continuity planning committee

The prime objective here is to establish the BCP committee required to:

- define the objectives, scope and key success factors of the business continuity process;
- manage the development of all required business recovery (BR) procedures for core business areas based on the business recovery timeline;
- support BR testing, reporting and maintenance;
- support and promulgate the required BR training and awareness programme;

BCP committee members must include nominated business recovery team managers and backups and a senior member from the recovery management team (RMT). The RMT is the team that resides at the pinnacle of the recovery management organization, generally managed by the CEO or backup.

Furthermore, the committee should approve the membership of the required business recovery teams and assign them to the project. A project manager should be appointed to co-ordinate the entire project (involving business and IT representatives). The project manager can appoint other project co-ordinators to control each core business function.

Once the overall project structure has been established by the committee, draft roles and accountabilities for all functions within the project will need to be established. Ideally, the people best suited to developing, implementing, testing and maintaining detailed BR procedures are those people who are responsible for supporting the core business function on a day-to-day basis.

It is also recognized that certain functions may be combined within teams rather than having separate teams for each function. The importance here is to ensure that all aspects of each core business function are covered.

Once developed, BR procedures will need to be tested and maintained on an ongoing basis. The focus should therefore be to ensure that the responsibility of the BR procedures is entrenched in the normal day-to-day duties of line functions.

BR responsibilities should be included in staff job descriptions so that associated recovery activities and tasks are recognized and catered for on an ongoing basis.

The BCP committee should also acknowledge and fully endorse the following:

- incorporation of BR material into orientation documentation for new employees;
- planned or unscheduled BR tests;
- the inclusion of overall business continuity strategy awareness and responsibilities in the performance reviews of managers and staff; and
- invitations of guest speakers and presentations to civil authorities (police, fire department, etc.) making them aware of the overall business continuity strategy and discussing with them any legal obligations that may require attention.

Table II
Unintentional threats

Cause	Effect
Accidental disclosure of data	Inadvertent disclosure of the organization's data, results, methods, plans, etc. to competitors via Internet or other means of electronic data transfer
Mechanical/supporting services failures, i.e. air-conditioning failure, UPS failure, backup generator failure, etc.	Effects on business processes/system availability. With regards to air-conditioning, i.e. legionnaires disease, refer to disease/epidemics
Backup and restore failure	Effects on system recovery timelines and the integrity of the overall disaster recovery process
Communication service loss	Impact of exchange failure or initial impact to telecommunications equipment
Disease/epidemics	Possible effects of closure of facility, quarantine, staff evidence of contaminated site
Earthquake/tremors	Possible loss of utility services, damage to sensitive equipment
Fire	Internal/external cause resulting in fire-related damage, including secondary effects, sprinkler, fire hose water damage, smoke damage
Flood/water damage	Includes burst water main, blocked drains, damaged roofs, etc.
Inadequate contingency	Effects of lack of or untested emergency response procedures, disaster recovery procedures/business continuity procedures
Lightning	Effects of direct and indirect lightning strikes on buildings, services, etc. likelihood of fire, power loss, power surges, etc.
Logical security mismanagement	Effects of poorly administered access requests
Power failures and electrical faults	Includes surges, sags, spikes, over/under volts, insufficient UPS power, etc.
Wind/storm	Possible loss of utility services

Perform the business impact analyses

A key step in protecting any organization is identifying potential risks/threats/problems as comprehensively as possible, and establishing methodologies for handling them within reasonable operating and economic constraints.

Business impact analyses can be applied to accommodate a single department, business unit or, ideally, the entire organization.

The methodology utilized should identify and evaluate the risks/threats and potential "problems" that could escalate into an unforeseen "disaster" impacting business services and functions, and/or technology systems.

The business impact analyses are a vital part of the planning process and, at a minimum, the objectives should be as follows:

- determine critical requirements (resources) and what impact an extended outage could have on business processes, staff and other areas within the organization;
- identify the target recovery time for each core business function and service;
- identify recovery priorities for core business functions and services;
- identify personnel, equipment and information needed to support the core business functions and services;
- identify potential "manual workarounds" in the event of extended outages;
- determine the monetary value of extended outages;
- provide relevant data into the BR project planning process, i.e. business impact charts and restoration orders, business recovery timeline, etc.;

- identify the need to commit personnel, time and other resources required to facilitate/design, develop, test and implement BR procedures;
- evaluate existing BR procedures and the likely points of failure, i.e. do not cater for extortion.

Once business impact analyses have been completed, findings should be consolidated and reviewed by accountable personnel. The appropriate levels of management will need to be provided with details of the findings and recommendations in the form of a business risk minimization action plan.

Executive management needs to recognize its responsibility for the business continuity function and its day-to-day implementation should be supported by an area accountable for the implementation of the business continuity process. This allocated area, on an annual basis, must also provide the appropriate levels of management with findings/recommendations from business impact and other risk analyses.

Along with the company directors, executive management is ultimately accountable for the integrity and functionality of the business and the welfare of its vital asset – staff.

Evaluate critical needs and prioritize business requirements

Critical needs are the necessary resources, procedures and equipment required to continue core business operations should facilities become inaccessible, key equipment become inoperable, key personnel become unavailable, etc.

For each core business function, the potential impact of a problem/crisis/disaster situation will need to be assessed to determine criticality as per requirements of a business impact chart and restoration order. This order should be standard in all corporate business recovery plans.

The recovery strategy should be based on providing minimum resources to ensure that core business requirements are fulfilled (e.g. the department concerned can maintain its core business activities in the interim and, at a later stage, reconstruct the department to its original state).

Determine the business continuity strategy and associated recovery process

In conjunction with the "risk reduction programme", the preceding steps have basically identified the core (business/department) functions and services and the target recovery times. These inputs will now need to be reviewed in identifying all associated costs and preparing a strategy to provide the initial restoration of core business functions. The objective of this process will be to analyse all the alternatives and strategies that are available to continue core business and associated IT functions and services.

Costs associated with new equipment, temporary facilities, etc., should be documented and recommendations presented to the BCP committee on the most feasible alternative from a cost/benefit analysis perspective.

A risk analysis of any proposed temporary site or backup site should also be undertaken. This will help to measure and identify any shortfalls that may exist with an organization's reliance on such a facility.

Consideration should also be given to the need for complying with regulatory requirements and maintaining the organization's public image. In relation to the latter, the loss of credibility and concern by shareholders, clients, etc. over the stability of the organization following a problem or crisis situation that is now out of control could lead to a reduction of market share and client/customer base.

Having established the exposure, via the business impact analyses on the one hand and the costs of eliminating or significantly reducing the exposures on the other, the BCP committee would have the necessary information to make specific decisions in relation to what safeguards to adopt or acceptance of the risk.

The business continuity process should be based on the business recovery timeline because: problems occur often; crisis situations occur occasionally; disasters occur rarely. It is practical to address the timeline within the overall business continuity planning process because events such as bomb threats, extortion, industrial relations, etc., although categorized as "problems", could escalate into a disaster situation.

Furthermore, the business continuity planning and implementation processes should comprise the following:

- *Objectives* – detailing the overall aim of the process, catering for disaster recovery of computer systems and business functions and services, and organization of business continuity, which ensures least impact to personnel and customers in a crisis and/or disaster situation.

- *Scope* – detailing the extent of coverage by the recovery process and "how" and "when" it will be invoked.
- *Logistics* – detailing the phases which relate to the disaster recovery process.

The scope will ensure the development of a workable model/methodology/plan which can then, with minor adjustments, be rolled out into other areas of the organization.

The objective is the implementation of an executive approved business continuity process for the entire organization, i.e. corporate business continuity process.

Prepare business continuity strategy and its implementation plan for executive management approval

Rather than attempting to address all areas of recovery simultaneously, a suggested approach is to target one or two key departments or core business functions and develop a BR manual based on the business recovery timeline. This can then be rolled out to all other areas of the organization.

This approach has the benefit of not having to commit too many resources to the project as well as allowing the strategies to be fully tested and proven workable. It also allows the staff to go through the learning curve and understand the full implications of the business continuity strategy and its associated recovery process.

Once the scope, objectives and key success factors, business continuity policy/standards, business recovery teams and their accountabilities have been defined by the accountable area, all details will need to be conveyed to the affected personnel.

In developing the overall implementation plan, the accountable area should identify the major tasks, related dependencies and responsibility assignments.

The assigned staff are not necessarily the people who would carry out all the work. They would be responsible for project managing their respective areas and would be accountable for ensuring the required activities are carried out, as well as monitoring and reporting on the progress.

The BCP committee will now be in a better position to comprehend the high-level strategy, the business continuity organization and its implementation.

The approved implementation plan is then utilized to monitor and track the progress with meetings held on a fortnightly basis during the initial stages. These meetings should be limited to feedback on progress only and details on progress presented to the committee.

Meetings requiring detailed discussions should be handled with the relevant personnel on an *ad hoc* basis.

Prepare business recovery plan

An outline of the BR procedures should be prepared to guide the collation of the required inputs. The committee may request to review and approve the proposed plan templates.

The benefits of such an approach are that it:

- helps to organize the detailed BR procedures;
- identifies all major steps before the writing begins;
- identifies redundant procedures that only need to be written once; and
- provides a road map for developing the BR procedures.

A standard format should be developed to facilitate the writing of BR procedures and the documentation of other information to be included in the plan. This will ensure that the BR procedures follow a consistent format and allows for ongoing maintenance.

Standardization is especially important if more than one person is involved in writing the procedures.

The BR procedures should be:

- developed based on the business recovery timeline and managed on project management disciplines – specialized software packages are available for this feature. Gantt Charts should contain recovery phases, activities which when completed achieve milestones, tasks subordinate to activities, durations. teams and dependencies;
- supported by a unique business continuity policy and associated standards (a policy on its own is inadequate) and include methods for maintaining and updating the plan to reflect any significant internal, external and/or business changes;
- structured using a team approach. Specific responsibilities should be assigned to the appropriate team. The structure of the recovery process and its personnel may not be the same as in the existing organizational charts. This structure is usually arranged around a team approach for major functional areas within the organization.

A relational database could also be utilized to ensure ease of update of recovery essentials such as telephone numbers, addresses, equipment types and models, etc.

The BR procedures will enable the continued operation of core business functions subsequent to either a prolonged disruption or disaster situation, and ensure the orderly resumption of all other supporting business activities in a specified timeframe.

As the data collection process concludes, all findings can be transposed into the appropriate recovery procedure templates or specialized recovery software.

Develop the testing criteria and procedures

The purpose of a BR test plan and strategy is to demonstrate the overall recovery ability of an area during a simulated major interruption of service(s) and to verify that the information in the BR procedures is correct.

The testing criteria and procedures are generally regarded as an excellent training mechanism for the personnel concerned and confirm that personnel understand their responsibilities and can perform them successfully. It is essential that the procedures be thoroughly tested and evaluated on a regular basis.

The test will provide the organization with the assurance that all necessary steps are included in the BR procedures.

Other reasons for BR testing include the following:

- determine the feasibility and compatibility of recovery facilities, BR procedures and supporting manual workarounds;
- identify areas in the BR procedures that need to be modified;
- provide training to the BR teams;
- demonstrate the ability of the business unit/department(s) to recover;
- demonstrate the ability of IT service providers to meet business expectations;
- provide motivation for maintaining and updating the BR procedures.

Test the business recovery process and evaluate test results

Below are a few recommended key activities which should be undertaken/initiated before, during and after the actual test by personnel responsible for the implementation of the business continuity strategy and associated recovery process.

On an ongoing basis:

- meet on a scheduled basis with members of each business recovery team to ensure they are fully aware of their BR responsibilities;
- facilitate the resolution of all concerns/issues regarding BR shortfalls and requirements;
- facilitate the development and ongoing maintenance of all BR procedures, and the completion of all required analyses;
- maintain all necessary BR guidelines and frameworks and a thorough understanding of the organization's varying environments;
- ensure that problem management, crisis management and disaster management processes are "linked".

During the test:

- meet with the relevant key area personnel within the organization and brief them about the test;
- facilitate the preparation of the test plan;
- perform the test, monitor the outcome; and
- complete the appropriate test log reports.

After the test has been completed:

- review the test log, noting all problems and identifying areas of concern within all processes involved;
- arrange a post-test meeting for the preparation of the test analysis and evaluation report;
- distribute the report to the committee members;
- if needed, initiate the appropriate problem resolution processes.

In the review process:

- on a scheduled basis complete a review of all major areas concerned, and prepare/submit the appropriate review findings to the BR planning team and the appropriate levels of management;
- facilitate the process of rectifying shortfalls/problems as identified the review.

Develop/review service level agreements

Service level management is the process of negotiating and defining the levels of service required from business activities and/or IT systems. This process includes reaching a service level agreement between two parties, i.e. user management and IT management, a balanced two-way agreement for the provision and use of a "service".

At a minimum, the following should be taken into consideration when seeking to develop a business recovery contractual agreement with an external business continuity service provider:

- Which type of agreement? i.e. contractual, reciprocal, written, verbal.
- What is the expiry date of the agreement?

- Who will be paying for the agreement to be in place and will the payment be charged out to other sectors of the organization?
- What are the formalities for cancelling the agreement?
- Will it be required that the participants must be notified of any changes to the hardware, software, facilities configurations and in the amount of computing time?
- Will the agreement specify BR/DR times, usage conditions, time allocation and sharing arrangements?
- Will the agreement list all the conditions and rules that must be followed when using the recovery facility?
- Will there be a commitment under the agreement to provide hardware and software which is missing or not compatible?

In regard to the IT disaster recovery component of a service level agreement, the following should be documented:

- recovery system, i.e. local area network
- restoration via backups;
- recovery teams;
- recovery procedures;
- recovery timeframe;
- restoration decision process;
- testing.

Update/revise the business recovery procedures and templates

Procedural maintenance provides for the continued updating of the procedures, assures that they consider and respond to all changes in the environment, keeps staff familiar with the business continuity strategy and recovery process, and provides for ongoing testing. The primary purpose of maintenance is to protect the departments from having to develop the procedures again.

Even though it is the responsibility of the owner to maintain it, certain personnel will have to be responsible for reviewing the procedures, i.e. audit, etc., thus ensuring that a workable recovery process is in place.

Periodic reviews should be conducted as specified and supported by the business continuity standards. Circumstances to trigger specific reviews include changes to the business environment, vendors, equipment and configurations, physical site, etc. On release of the new version(s), it is imperative that additional copies are despatched for offsite storage.