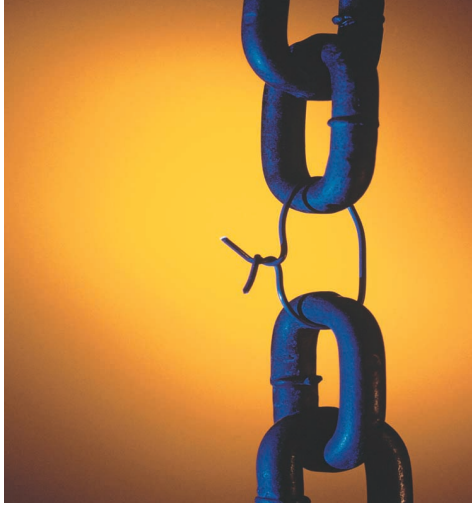


Will your business keep running if disaster strikes? Following the eight steps of the business continuity planning cycle can help you be prepared.

Wing Lam

Ensuring Business Continuity

Last year's terrorist attacks in the US have forced many organizations to critically reevaluate the adequacy of their existing business continuity plans and disaster recovery arrangements. The tragedy highlighted how important it is for organizations to remain commercially operational under even the most exceptional circumstances. E-business, which relies heavily on IT, is particularly vulnerable, because IT failures directly limit the capability to generate revenue.

The thoroughgoing approach to business continuity planning (BCP) that I present here—called the BCP cycle—can help you avoid those pitfalls. The BCP cycle is generic enough to have practical value in a wide range of IT-related organizations, and it is process-oriented, ensuring well-guided BCP efforts and tangible results.

BUSINESS CONTINUITY PLANNING CYCLE

BCP is a cyclical process; an organization should review its business continuity plan whenever it introduces changes to the business or alters its business priorities. I see the BCP process as a cycle of eight core steps, as depicted in Figure 1.

Figure 1 (next page) shows two concentric rings. The inner ring describes the core BCP process. Inseparable from BCP is the concept of business *recovery* planning (BRP). Even when an organization can ensure business continuity, typically with backup resources, at some point it must also recover its previous, fully functional state. The outer ring depicts the BRP process. As an organization works through each core BCP step, it must, at the same time, address BRP.

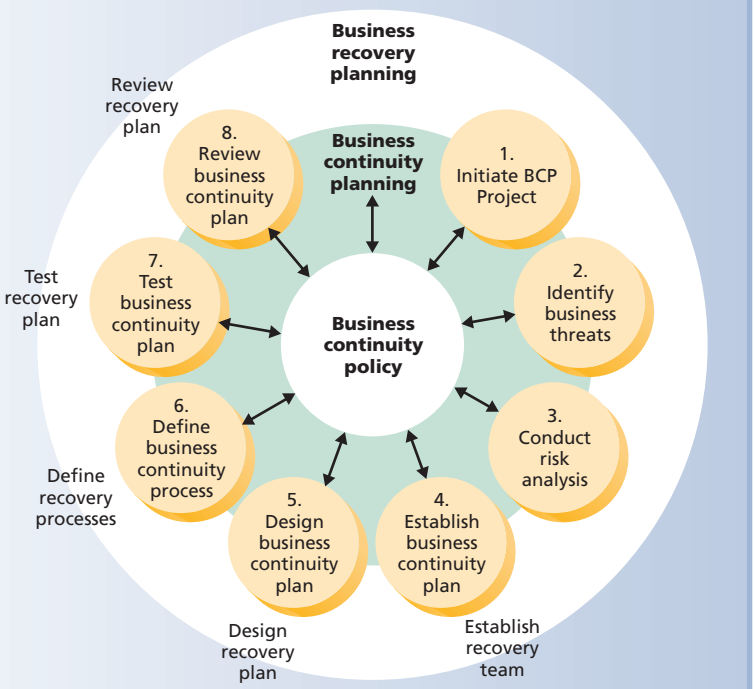
Central to the BCP cycle is the business continuity policy, which defines the organization's holistic approach to business continuity. The key areas covered in a good business continuity policy include

- *contact points*—who to contact during office hours, outside office hours, and in an emergency;
- *roles and responsibilities*—a well-defined organizational structure for the business continuity and recovery teams;
- *risk levels*—a categorization of business risks and the level of risk the organization deems acceptable;
- *continuity and recovery service levels*—how much time is acceptable for responding to threats, implementing continuity plans, and recovering from failure scenarios;
- *business continuity reviews*—how and when the organization reviews business continuity plans;
- *business continuity processes*—processes and procedures that inform staff how to react to and handle particular failure scenarios;
- *incident reporting and documentation*—methods of recording and documenting incidents and responses to them;
- *testing*—acceptance criteria and testing requirements for the business continuity plan; and
- *training*—training requirements for staff involved in business continuity and disaster recovery processes.

An organization can gradually compile its business continuity policy as it works through the BCP cycle's eight core steps. However, the policy

1520-9202/02/$17.00 © 2002 IEEE

Figure 1. BCP cycle.



should remain a living document that you maintain during each cycle.

EIGHT STEPS

Now let's look at the BCP cycle's eight core steps in more detail.

Step 1: Initiate the BCP project

1.1 Obtain and confirm support from senior management.
1.2 Identify key business and technical stakeholders.
1.3 Form a business continuity working group.
1.4 Define objectives and constraints.
1.5 Establish strategic milestones and draw up a road map.
1.6 Begin a draft version of business continuity policy.

It goes without saying that senior management support and buy-in is essential before starting the BCP effort. To kick off the project, establish a business continuity working group and give it specific objectives to work toward—defining the strategic milestones for BCP, for example. Empower the group by including key business and technical stakeholders who have the decision-making authority to make it happen.

Consult within the group and with senior management on strategic milestones and constraints. (For example, when do you need a full business continuity plan? Can it be phased in? Are there any specific regulatory requirements? What is the approximate budget?) Draw a road map to guide the organization. Get the working group to start an early draft of the business continuity policy; even though the document will be incomplete, it will help steer the group toward the issues that need attention.

Step 2: Identify business threats

2.1 Identify the community of business and technical stakeholders.
2.2 Conduct threat identification workshops.
2.3 Delineate and document business threats.

IT-based organizations generally rely on three types of resources—technology, information, and people. Consider what threats can render these resources either unavailable or inaccessible.

- *Technology threats* include natural disaster (such as flooding), fire, power failure, systems and network failure, systems and network flooding (when attackers try to overwhelm a network with traffic), virus attack, denial-of-service attack, theft, vandalism, and sabotage.
- *Information threats* come from hacking, theft, fraud, fabrication, alteration, misuse, natural disaster, fire, and the degradation of the ink on paper records.
- *People threats* include illness, recruitment shortfalls, resignation, compassionate leave, pregnancy, weather, and unavailability of transportation or office access.

In particular, use workshops to tease out the nonobvious threats and those specific to your particular industry sector. For example, the financial services and banking sectors work under strict regulations concerning financial auditing and the retention of audit logs. Delineate and document the business threats.

Step 3: Conduct a risk analysis

3.1 Conduct risk analysis workshops.
3.2 Assess the likelihood and impact of threat occurrence.
3.3 Categorize and prioritize threats according to risk level.
2.4 Review outputs of risk analysis with management.
3.4 Ascertain level of risk acceptable to the organization.
3.5 Document outputs in business continuity policy.

Risk is a factor that considers the likelihood of a threat actually occurring and its consequences in terms of finan-

cial loss, loss of customer confidence and business partnerships, and damage to reputation.

A threat's likelihood of occurring can be classified as either almost certain, likely, moderate, unlikely, or rare. Consequences can be catastrophic, major, moderate, or minor. Most organizations find it adequate to categorize and prioritize risks as high, medium, or low. Your high risks are threats that are almost certain or likely to occur and would result in catastrophic or major consequences. (Historically, terrorist attacks have been considered low risk, because their likelihood was considered rare even though their consequences could be catastrophic. Given recent events, however, upgrading their risk rating is reasonable.)

Seek out the level of risk acceptable to your organization—which threats are you prepared to ignore because either their consequences or their likelihood are too low or insignificant?

Consider which threats to ignore because either their consequences or likelihood are too low or insignificant.

Step 4: Establish the business continuity team

4.1 Identify key business, technical, and customer services stakeholders.
4.2 Form and empower the business continuity team.
4.3 Clarify and agree on team objectives and working mode.
4.4 Define roles and responsibilities; produce a work plan.
4.5 Identify incident engagement and response processes.
4.6 Update business continuity policy.

When an incident does occur, a business continuity team must be ready to engage and manage the incident and to enact whatever business continuity plans are in place. Form the business continuity team and establish clear objectives. Define roles and responsibilities, and assign roles to specific individuals. Ideally, compose the team of individuals who hold existing roles of responsibility—they will be most familiar with existing business and IT practices.

Several roles are typical of business continuity teams.

- A *business continuity manager* is the first point of contact, manages the incident, initiates the business continuity plan, mobilizes the business continuity team, and presents key decisions to business owners when appropriate.
- The *business owner* makes key decisions about how the business handles incidents.
- The *technical services manager* manages disruptions to technical services, such as IT infrastructure and applications; initiates continuity arrangements; and interacts with third-party business continuity service providers.
- An *estate manager* manages disruptions relating to buildings, offices, and the surrounding environment; initiates continuity arrangements and interacts with third-party business continuity service providers.
- The *business operations and customer services manager* manages disruptions to business operations and customer services; keeps customers informed if there is a noticeable impact on customer service levels; initiates continuity arrangements; and interacts with third-party business continuity service providers.
- *Business continuity (or resumption) teams* are technical, estate, or customer services teams that execute the business continuity plans.
- A *recovery manager* guides the business' recovery to normal operations.

With a well-formed business continuity team, the working group can take more of a steering role. Get the business continuity team to think about the processes it must follow to engage, respond to, and manage incidents. The team should also decide how it will coordinate activities between team members.

Step 5: Design the business continuity plan

5.1 Identify critical and noncritical business services.
5.2 Establish preferred business continuity service levels and profiles for continuity and recovery.
5.3 Reaffirm key constraints (such as time and cost).
5.4 For each threat, identify possible continuity strategies and evaluate them in terms of time, cost, and benefits.
5.5 Identify and engage potential business continuity partners.
5.6 Draft a set of continuity plans and work toward an agreed set of plans with senior management.
5.7 Produce and execute an implementation plan.

If you haven't already considered this, now is the time to determine your desired business continuity service levels. Two key metrics are

- *business resumption response time*, the time taken before your organization can continue with business after an incident or failure scenario; and
- *recovery time*, the time taken for an organization to fully recover its original state after an incident or failure scenario.

You can sensibly apply these metrics at the business services level. For example, let's say business services 1 and 2 are critical; they therefore need shorter business

Table 1. Typical to worst-case scenario analysis.

Resource type	Business threat	Failure scenario	Business continuity strategy	Evaluation
Technology	Systems failure	Typical: Failure affects some servers; repair time is short (hours or 1 to 2 days).	A1: Have a third-party maintenance and support agreement.	Cons: Suffer business consequences while servers are not in operation.
			A2: Have an emergency third-party support agreement with guaranteed on-site response time.	Pros: Faster repair time. Cons: Suffer business consequences while servers are not in operation.
			A3: Have redundant servers on cold, warm, or hot standby.	Pros: Minimal server down time. Cons: Purchase and maintenance costs for additional hardware and software.
			A4: Combine options A1 to A3.	
		Worst case: Failure affects all servers, and repair time is lengthy (many days or weeks).	B1: Have a secondary or disaster recovery site for redirected Internet traffic.	Cons: Expensive, requires alternative site and replication of infrastructure and environments.
Information	Hacking	Typical: Attackers compromise a server, disrupting or terminating applications and processes.	C1: Have support arrangement to conduct system cleansing; restart or restore application and processes on the server.	Pros: Relatively cheap.
			C2: Have redundant servers on cold, warm, or hot standby.	Pros: Minimizes disruption. Cons: More expensive, requires purchase and maintenance of additional hardware and software.
		Worst case: Attackers compromise a server, removing or altering sensitive information.	D1: Restore information from the last database backup.	Cons: Suffer business consequences during restoration.
			D2: Write all data to a second database; restore from that database.	Pros: Lost or altered information can be quickly restored. Cons: More costly, requires additional data source management.
			D3: Restore information from audit trails.	Cons: Can be tedious and time-consuming.
			D4: Combine D1 to D3.	

resumption response and recovery times than noncritical business services 3 and 4.

Continuity and recovery profiles indicate how soon a particular business must resume and recover certain services; in short, these profiles define the requirements that the business continuity plan must meet.

To identify failure scenarios and possible business continuity strategies for each type of threat, you can use a typical and worst-case scenario analysis. Table 1 shows this kind of analysis for an e-business system

Use scenario analysis to help understand the relative pros and cons of individual business continuity strategies. Common strategies are available for each of the three resource types.

- *Technology.* Redundancy (of hardware and network, for example), maintenance and support agreements, and backup and restore capabilities are common defensive strategies.
- *Information.* Recover information by using data mirroring, backup and restore, auditing, and off-site or secondary data storage.
- *People.* To temporarily shore up people-related resources, use contract staff, rotas (workloads that a company can change in response to business demand or personnel shortfalls), call-out arrangements (having certain staff in standby mode to be called to work as necessary), rental offices and sites, manual procedures, and service-forwarding agreements (such as with specialist call centers).

Business continuity must consider a disruption's effect on three types of resources—technology, information, and people.

The choice of business continuity strategies often affects a system's overall design—a strong argument for considering BCP as an integral part of your IT development process. In evaluating individual business continuity strategies, include the following criteria:

- costs for acquisition, deployment, testing, training, and associated management overhead;
- level of protection;
- business resumption response time; and
- time to implement, including time for acquiring, deploying, and testing the business continuity strategy and for conducting relevant and necessary training.

Examine the tradeoffs between strategies. Less-expensive strategies typically have greater limitations and often can't handle worst-case scenarios.

Explore potential business continuity partnerships. For example, several companies specialize in off-site data storage; a growing number provide complete business continuity and recovery services. Work toward an agreed set of business continuity plans with senior management. Produce and execute an implementation plan for putting the business continuity plan and strategies in place.

Step 6: Define your business continuity processes

6.1 Identify, define, and document business continuity processes.
6.2 Review and verify business continuity processes with relevant stakeholders.
6.3 Identify training requirements.
6.4 Develop training exercises, role-playing scripts, and simulation case studies.
6.5 Initiate training and awareness programs.

Business continuity processes include

- handling specific failure events, such as fire and network failures;
- backup and restoration of systems and business data;
- virus management;
- incident reporting;
- problem escalation hierarchies;
- customer and staff communication; and
- contact procedures for third-party support providers.

Step 6 is about fully documenting these business continuity processes to prepare your organization for any kind of incident. Communicate these processes to the relevant parties. Ensure that the team has identified training requirements and has followed up with a training program for relevant personnel.

Step 7: Test your business continuity plan

7.1 Define business continuity acceptance criteria.
7.2 Formulate the business continuity test plan.
7.3 Identify major testing milestones.
7.4 Devise the testing schedule.
7.5 Execute tests via simulation and rehearsal; document test results.
7.6 Assess overall effectiveness of business continuity plan; pinpoint areas of weakness and improvement.
7.7 Iterate tests until the plan meets acceptance criteria.
7.8 Check, complete, and distribute business continuity policy.

There are at least four important reasons for testing your business continuity plan. You want to

- validate the plan's effectiveness in meeting your stated business continuity service levels;
- identify, at an early stage, any shortcomings in the plan;
- assess whether your business continuity service levels are realistic and achievable given your budgetary and time constraints; and
- give senior management and other parties (such as regulatory bodies) confidence in the plan.

Table 2. Common pitfalls in the business continuity planning process.

Pitfalls Plans can be …	Description
Incomplete	The BCP process is not complete. Outputs such as the business continuity plan and policy either do not exist or exist in incomplete form.
Inadequate	The plan and strategies can't deal with the level of risk that the organization deems acceptable.
Impractical	The plan is not practical or achievable within the organization's constraints (manpower, time, and budget, for example).
Overkill	The plan is overly elaborate or costly with respect to the overall level of business risk that the organization is willing to take.
Uncommunicated	The business continuity team has not communicated the plan to all the right people. Staff—both management and technical—remains unaware of business continuity issues.
Lacking a defined process	Business continuity processes remain ill defined. Staffers are unsure of how to react in a failure scenario, or they discover too late that their existing processes fall short.
Untested	The organization hasn't tested its plan, or hasn't tested it thoroughly enough to provide a high level of confidence in its soundness.
Uncoordinated	The business continuity effort lacks organization and coordination. The organization has either not established a business continuity team, or the team lacks individuals who can effectively drive the effort to completion.
Out of date	The plan hasn't been reviewed or revised in light of changes in the organization, its business, or technology.
Lacking in recovery thinking	The organization doesn't adequately address how it intends to recover to a fully operational state after executing its business continuity plans.

Formulate a business continuity test plan that identifies individual business continuity tests. A typical to worst-case scenario analysis can serve as a starting point in identifying the failure scenarios you should simulate and test. Bear in mind that business continuity testing can take considerable time to complete—one to two months is not uncommon for a large-scale e-business doing this for the first time. When devising the test schedule, consider the disruption and time out that the testing will cause other activities.

Review your test results to validate the business continuity plan and pinpoint any shortfalls either in the plan itself or in its execution. Repeat the testing until your plan meets acceptance criteria.

Step 8: Review your business continuity plan

8.1 Develop a review schedule for different types of review.
8.2 Arrange a business continuity review meeting or workshop.
8.3 Update the business continuity document.
8.4 Kick off another BCP cycle if necessary.

The last core step in the BCP cycle highlights the fact that the organization must review its business continuity plans whenever any of the following occurs:

- significant changes to the business—for example, the launch of new e-business operations;
- changes in business priorities;
- shifts in the legal or regulatory landscape;
- significant world events (wars or terrorist attacks);
- changes to the IT budget;
- physical relocation of IT systems and operations;
- outsourcing of IT systems and operations;
- developments in IT infrastructure; and
- significant changes in the labor market.

Reviews take many different forms. For major reviews, independent experts—typically from specialist business continuity firms—can perform a thorough and detailed examination of your plans. For less substantial reviews, an internal process might suffice, particularly when participants have prior business continuity experience.

If a review suggests that the current business continuity plan needs significant revisions, it's time to kick off another cycle of BCP.

COMMON BCP PITFALLS

Unfortunately, organizations without a systematic approach to BCP are more likely to end up with plans that are either inadequate, incomplete, or impractical. Table 2 describes some of the typical ways these plans go awry.

MAINTAINING BCP AWARENESS

Contrary to the way businesses often treat it, BCP is not an on/off event. BCP is an ongoing concern that should be a high priority for every organization, but especially those running 24-hour e-business operations 365 days a year. You can do several things to keep BCP on the management agenda:

- Explicitly identify business continuity requirements up front. Actively manage and track their fulfillment as part of the business design and systems design processes.
- Emphasize business continuity as one the core principles in designing e-commerce and IT solutions.
- Frequently refer to high-profile incidents as reminders of what can happen without a business continuity plan.
- Create a specific role for a business continuity manager within the organization or project structure.
- Hold business continuity awareness workshops. For maximum and lasting impact, get an external expert to facilitate such workshops.
- Hold regular, must-attend BCP review meetings.
- Include business continuity in formal training for both technical staff and management.

Having a good business continuity plan is like having insurance: you hope you don't have to use it, but you reap the rewards when you do. Can your organization afford not to have one? ■

Wing Lam *has worked for several large consulting firms on large-scale systems design, project management, and IT strategy. His most recent projects include a financial services Internet portal, an Internet bank, a B2C shopping mall, and a B2B exchange. He is an associate at the Institute of Systems Science, Singapore. Contact him at wlam_uk@yahoo.com.*

For further information on this or any other computing topic, visit our Digital Library at http://computer.org/publications/dlib.