Business Continuity Planning Checklist: The Top 10 Best Practices

Table of Contents

Business Continuity Planning Checklist: The Top 10 Best Practices 1

1: Put Together a Business Continuity Planning Team 2

2: Identify Business Processes and Operations 3

3: Conduct a Thorough Risk Assessment 3

4: Define Your Organization's Strategic Response 4

5: Generate Business Continuity/Disaster Recovery Plans 5

6: Train Staff to React Flexibly to Risk and Recovery 7

BEYOND BUSINESS CONTINUITY PLANNING: BUSINESS CONTINUITY MANAGEMENT SYSTEMS 8

7: Develop a Business Continuity Test Plan 11

8: Deploy Continuity/Disaster Recovery Capabilities 12

9: Monitor, Manage and Maintain Your Continuity Plan 13

10: As Appropriate, Coordinate Activities With Others 15

SPONSORED BY IBM

> "In preparing for battle I have always found that plans are useless, but planning is indispensable." —***Dwight D. Eisenhower***

Every organization, large and small, needs a business continuity plan — a blueprint for keeping the business operational in the face of disruption or disaster. This is perhaps an oxymoron: After all, most companies already have a business continuity plan.

But wait. Do you have a plan that's gathering dust on a shelf or on an archive server — or do you have an up-to-date plan that you know will actually work? Is your plan well thought out — or was it backhanded quickly? When was the last time you tested the plan?

Is your business continuity plan considered in your change management efforts? Has anyone reviewed the plan lately with an eye to using newer capabilities such as electronic vaulting to improve continuity and recovery while reducing costs?

Ah, so many questions. Perhaps too few answers. As you consider the state of your business continuity plan, take a look at these best practices to see how your organization is doing.

68% of respondents work in organizations that have implemented Internet security measures. (AT&T 2007 Business Continuity Survey)

☑1 *Put together a business continuity planning team capable of thinking out of the box.*

These people will generate/update your organization's BC plan with strategic mandates in mind. They may also be key players if and when disaster/failure/discontinuity occurs, at which time their ability to respond agilely to circumstances will be crucial. Depending on the size of your organization, you might want to create both an oversight group and a core BC/recovery team.

You'll need to assign areas of responsibilities and establish a chain of command, keeping in mind that some disasters/failures might inhibit access to personnel (so you'll need to assign alternates).

Because full recovery can take a while after the immediate crisis ebbs, you should create a recovery team comprised of specialists (security, IT, communications, personnel, etc.) who can work with emergency and government agencies. The team will need appropriate equipment, too — such as flashlights, protective clothing, satellite phones.

59% **of respondents indicate their organization has established redundant servers and/or backup sites.**
[AT&T 2007 Business Continuity Survey]

☑2 *Identify business processes and operations that are critical to your organization and the ways in which various disaster, failure or discontinuity scenarios would affect them.*

This impact analysis should be done in terms of your organization's strategic goals rather than in terms of specific systems or organizational structure, and the key question to be answered is: What facilities and processes are critical to the survivability of the business?

57% **of respondents say their organization educates employees about business continuity.**
[AT&T 2007 Business Continuity Survey]

☑3 *Conduct a thorough risk assessment.*

… Again, strategically: What's at risk first? Your risk assessment should identify those functions, processes, resources and suppliers most critical to your organization's operations. It should also articulate the vulnerabilities and risks each of these faces — including threat probabilities. As appropriate, you may want to conduct separate risk assessments for specific mission-critical areas of the business. Questions that need to be answered include:

- What's the potential cost of downtime for various processes? What's the potential cost of total business failure?

- What are acceptable levels of service during recovery? What service-level agreements or other performance metrics must be met to avoid breach of contract?
- In what priority do processes need to be maintained/restored to sustain business operations?
- Which employees are essential? What other resources (service providers, etc.) are essential?
- How would a failure affect ability to meet compliance mandates?

41% of respondents' organizations have not tested their business continuity plan in the previous 12 months.
[AT&T 2007 Business Continuity Survey]

☑4 *Define your organization's strategic response to disaster/failure/discontinuity — prioritizing operational performance goals.*

This can be articulated in terms of corporate-level, process-level and resource-level responses, including funding. Don't forget plans for employee availability, alternative work processes, possible pre-positioning of critical resources, and communication with customers. Among the questions to be answered:

- Should critical processes be decentralized? Is there a need for dual processing centers? Is the distance between alternate locations sufficient?
- What recovery time objectives should be established?
- How effective are existing disaster recovery plans, policies and procedures? How effective are existing data backup and recovery policies and procedures?

☑5 *Generate business continuity/disaster recovery plans to ensure that critical operations continue to function.*

These blueprints should describe the scope of the plan, documenting requirements in detail, and include updates to existing plans as well as any missing capabilities that need to be implemented so your organization can be as prepared as possible. A staff training plan should also be devised. Your plan should address such elements as:

- *An employee contact plan* that establishes who needs to be reached with what information, provides business-critical employees with out-of-band means to communicate, includes a mechanism for keeping the plan up to date, and ensures that employees know how to get information about when and where to return to work.

- *Awareness of the business continuity plans of suppliers and partners*, including assurance that their plans are sufficiently complementary to your own.

- *Offsite data backup at a secure location sufficiently distant from your data center(s)*, including procedures for storing critical data (not just business data but also application code, etc.) on removable media. Make sure key personnel have the means (passwords, keys to the facility) to access it all so they can restore operations as soon as possible.

- *Power backup*. Most disasters are small in scope. But if your data center is offline because of an errant backhoe down the street, your mission-critical operations are still threatened. Your plan should include contingencies for both short-term and long-term power outages.

- *Alternative communications*. Regional disasters can make communication by normal means erratic or impossible. Among the alternatives to consider: employees' personal e-mail addresses, their personal cell phones, ham radio, satellite phones.

30% of respondents say that business continuity planning is not a priority.
[AT&T 2007 Business Continuity Survey]

- *Alternate site of operations*. Your plan should include an alternative in case key structures are rendered unusable — such as a branch office, which should be prepared in advance for such a contingency.

- *Equipment and services replacement*. Your plan should include mechanisms for replacing equipment that's been damaged.

58% of business functions, on average, are considered mission-critical.
[*Gartner/Disaster Recovery Journal* October 2005 survey http://www.drj.com/articles/fall06/1904-03p.html]

☑6 Train staff to react flexibly to risk and recovery.

Remember: At least some of the procedures that are likely to work best during a disaster will probably be developed during the disaster — existing processes, protocols and procedures may well be ineffectual. Staff must therefore be trained to respond flexibly and innovatively in a strategic way to cope with risks and disasters.

What matters isn't a particular system or process but the larger strategic goal (e.g., serve the customer). These goals should already be articulated (See Best Practice #4), and the organization's assets (internal and external, physical and intellectual), as well as what may have an impact on them should already be identified (See Best Practices #2 and #3).

BEYOND BUSINESS CONTINUITY PLANNING:
BUSINESS CONTINUITY MANAGEMENT SYSTEMS

"Business continuity programs … are most effective when grounded in generally accepted standards and built according to the business's objectives," write Susan Yardis, Robert Giffin and John DiMaria in *How to Deploy BS 25999**.

The movement toward business continuity standardization is now under way. Emerging from it are "business continuity management systems" (BCMS) and British Standard 25999, an internationally accepted standard that describes a mature, repeatable business continuity program based on objective metrics.

BS 25999 matters not just because it can help organizations develop and implement internal business continuity plans, but also because it smoothes business-to-business and business-to-customer planning by providing a common language and an overarching conceptual framework.

That framework, says DiMaria, who is the British Standards Institution's Americas product manager of business continuity, can be explained in terms of what it does, its benefits and its expected outcomes.

What BS 25999 Does

Comprised of a code of practice (consistent with ISO 17799) and a specification (consistent with ISO 27001), BS 25999 involves two phases: development of a BCMS, and implementation and operation of a BCMS that together can:

> Proactively improve resilience against the disruption of an organization's ability to achieve key objectives.

> Provide a rehearsed method of restoring an organization's ability to supply its key products and services to an agreed level within an agreed time after a disruption.

> Deliver a proven capability to manage a business disruption and protect the organization's reputation and brand.

The Outcomes and Benefits

BS25999 delivers what one would expect from a business continuity plan:

> Identifies and protects key products and services, ensuring their continuity, and proactively identifies the effects of an operational disruption.

> Enables an effective incident-management capability, minimizing impacts on the organization through effective response.

> Maintains an ability to manage uninsurable risks.

> Methodically develops and documents the organization's understanding of itself and its relationships with other organizations, relevant regulators and government agencies, local authorities and emergency services providers.

> Trains employees to respond effectively to an incident or disruption, encourages cross-team cooperation and demonstrates credible response via exercising (testing) processes.

BS 25999 has been welcomed because it codifies generally embraced best practices. And as time passes, it may become incorporated into regulatory mandates.

* *How to Deploy BS 25999*, by Susan Yardis and Robert Giffin, Avalution Consulting, and John DiMaria, BSI Management Systems America [http://www.avalution.com/PDF/How_to_Deploy_BS_25999.pdf]

7 Develop a business continuity test plan.

To make sure that they actually work, business continuity plans must be tested frequently and in as realistic a manner as possible. Many aspects of a business continuity plan should undergo testing, so your test plan should include simulations as well as actual recovery implementations, all of which should be documented and logged.

Varying what and who gets tested prevents the testing process from getting stale and ensures that there's widespread understanding of recovery procedures. Once the test has been completed, all the issues it has uncovered should be reviewed and resolved.

How often should your plan be tested? Most experts say at least once a year. Some say every six months. Others believe testing should be an ongoing process.

90% of organizations plan for a single-facility outage.

(Gartner/Disaster Recovery Journal Online 2005 survey, http://www.drj.com/articles/online/2005/1904-01.pdf)

8 Deploy necessary business continuity/ disaster recovery capabilities.

Several technologies can improve the effectiveness of business continuity plans. This is important at a time when 24x7 information access and transactional ability make a huge competitive difference.

- *Server replication*. Using an IP connection, server replication provides a reliable secondary infrastructure with automated replication and failover processes that's able to maintain the continuous availability of data and applications. This minimizes data loss and downtime.
- *Storage replication*. Critical data is mirrored in real time (or near-real time) at a secure remote location, regardless of host environment, making resumption of operations quick and easy compared with traditional storage options.
- *Electronic vaulting*. Selected files are automatically backed up at scheduled frequencies and times, and any changes are captured, compressed, encrypted and transmitted, usually via an IP connection, to a secure remote facility.

68% of organizations plan for a regional disaster.

[*Gartner/Disaster Recovery Journal* October 2005 survey http://www.drj.com/articles/fall06/1904-03p.html]

9 *Monitor, manage and maintain your business continuity plan.*

Organizations change quickly. It's important to make sure that all elements of your organization continue to comply with BC policies and procedures. You also need to keep your BC plan up to date in terms of systems, networks, facilities, staff, processes and priorities. Toward that end, create a BC plan update process — one that continuously reflects organizational changes.

62% of organizations plan for an IT outage.

[*Gartner/Disaster Recovery Journal* October 2005 survey http://www.drj.com/articles/fall06/1904-03p.html]

Expect to update your business continuity plan after each test. The plan should also be reviewed and altered as necessary whenever relevant business changes occur. This makes business continuity planning part of your organization's change management process. Anytime new applications are being designed or deployed, anytime hardware is upgraded or replaced, anytime business processes are being revamped, the impact on your business continuity plan must be addressed.

☑10 As appropriate, coordinate your activities with others.

Share your plans with local governmental agencies, building management, community leaders and partners/suppliers. The training of your recovery team should include familiarizing them with various agencies and those agencies' capabilities, practices and procedures during various types of disasters.

50% of organizations plan for a key service provider failure.

[*Gartner/Disaster Recovery Journal* October 2005 survey, http://www.drj.com/articles/fall06/1904-03p.html]

SPONSORED BY IBM.

Produced by
Minnick Web Services, LLC