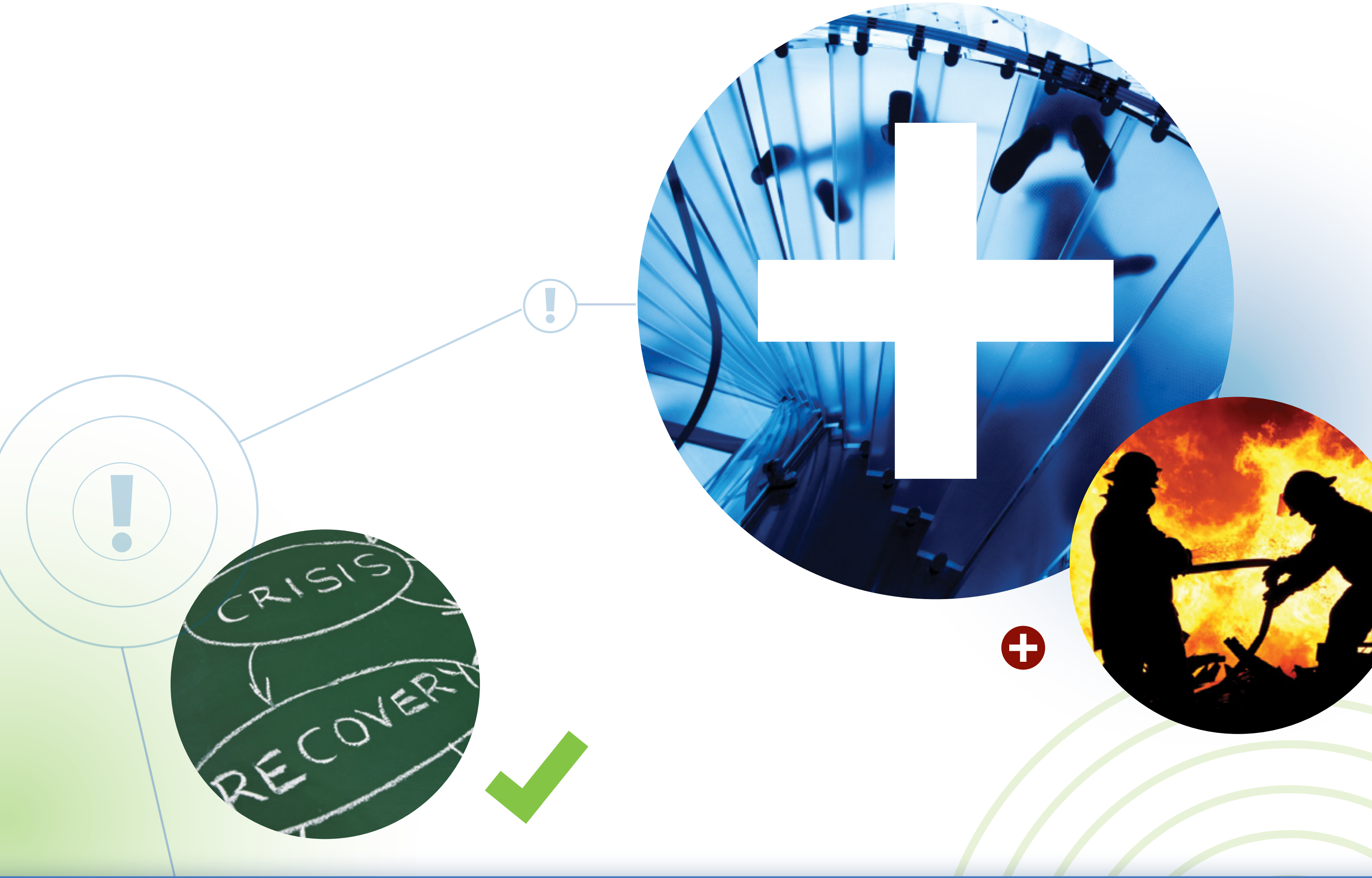
ONSOLVE™



The Definitive Guide to BUSINESS CONTINUITY PLANNING

Greg Livingston, ABCP, CDRP

Welcome to the *Definitive Guide to Business Continuity Planning*—the indispensable resource for developing your business continuity plan.

This handbook can be used to guide you in developing a BC plan from start to finish, or as a tool to test and improve your existing plan, or for anything in between. We've organized it so it's easy to find the information that matters most to you. Use the table of contents in each section to help you home in on just what you need at any one time. Here's a brief overview of the five chapters:

Chapter 1: Contingencies: Does your plan cover all bases?

This is where to start if you haven't begun to develop your plan. We'll explore the risks vs. rewards of developing a plan and show you how to evaluate the impact of threats on your business. You'll learn how BC plans have developed and improved over the years and why they've become standard, and why everyone at every level in your company should support the development of your own, customized plan. Use this chapter to determine who should be on your planning team, what regulations must be satisfied for your industry and what kind of threats you should prepare for.

Chapter 2: Business Impact Analysis: The all-important foundation

Here you'll learn all about the business impact analysis (BIA). We'll explain the most important elements of a BIA, how to pull together the information needed and help you determine if and when it's time to hire a professional rather than do it internally. Set aggressive yet realistic goals for recovery and understand the difference between the RTO (recovery time objective) and the RPO (recovery point objective).

Chapter 3: Think it Through: Effective strategy, development and documentation

Once you've completed your risk assessment and your BIA, you're ready to start planning recovery strategies. This section provides a graphical recovery continuum and will show you a recovery strategy development process that works department-by-department. You'll find useful templates and advice on writing procedures that are tailored to the skill sets in your company. We'll explore manual procedures, technical procedures, alternate worksites, staffing issues, incident response and crisis communication.

Chapter 4: Your BC Toolkit: Options and integration

Once you know what your plan will cover, you need to figure out the best tools to put into place to document, distribute and enact it. To do that, you'll need to carefully consider your corporate culture, its values and its unique show-stoppers. From there we'll explore the tools for preparing your plan and managing an event, determining which tools are best for you.

Chapter 5: The Final Countdown: Rollout, testing, and results

If you've documented your BC plan, you must establish a schedule to test it regularly and update it frequently. This section has tips on keeping your plan current and for testing not only your plan, but also your vendors and anyone else who would be critical to your business recovery. You'll learn how to initiate a variety of tests and explore the benefits and limitations of each.

Contents

Chapter 1: Contingencies: Does your plan cover all bases? 4
- BC planning: are all your bases covered? 6
- BC planning defined 8
- BC planning methodology 13
- Some BC best practices 19
- Summary 20

Chapter 2: Business Impact Analysis: The all-important foundation 21
- What exactly is a business impact analysis (BIA)? 23
- Why you must do a BIA 23
- Prerequisites for a successful BIA 25
- Data gathering 26
- Impact assessment 27
- Recovery requirements 28
- Completing a BIA matrix 30
- Finalize your BIA 30
- Summary 30

Chapter 3: Think it Through: Effective strategy, development and documentation 31
- Recovery strategies 33
- The recovery strategy development process 34
- Incident response 36
- Crisis communication 37
- Developing the plan 38
- Summary 39

Chapter 4: Your BC Toolkit: Options and integration 40
- What to expect from a tool 42
- Summary 46

Chapter 5: The Final Countdown: Rollout, testing, and results 47
- Disaster strikes 49
- Checklist test 56
- Structured walk-through test 57
- Recovery simulation 59
- Recovery simulation – information technology 60
- Communications test 62
- Summary 63

1

2

3

4

5

CHAPTER 1

Contingencies: Does your plan cover all bases?

Contingencies: Does your plan cover all bases?

CHAPTER 1

Situation

An interruption to daily operations is not just costly—it can tarnish your reputation, open the door to competition and threaten the well-being of your staff. Interruptions run the gamut in severity, likelihood and impact, from natural disasters and terrorist threats, to something as simple as a backhoe operator taking out your fiber optic cable. No matter what size or industry your business is, you must be prepared for interruption.

In the aftermath of the September 11, 2001 attacks on the World Trade Center, while many businesses were subsequently wiped out, those companies with a comprehensive BC plan in place were able to get up and running again in days. Thanks to the increasing implementation of BC planning, organizations all over the world are more successfully safeguarding lives, assets, revenues and value.

Need

BC planning involves an investment in time, technology, tools, consulting and training. It's an ongoing process, requiring regular evaluation, revision and practice. It's a relatively young discipline and expertise and standards are still being developed. And despite the copious news of everything from cyber attacks to volcanic eruptions wreaking havoc on businesses, top management is still notoriously difficult to motivate to invest in BC planning.

Solution

Recognizing the need for BC planning and tools, in the early 1990s governments and industry associations started developing comprehensive statutes, regulations and guidelines. BC planning is now its own industry that includes data backup, hot-site and telecommunications providers, BC software tools, consulting companies, and dedicated publications.

Results

This chapter will introduce you to BC planning, beginning with a risk assessment. As you work your way through this book you'll be guided through all the phases of developing your own effective BC program.

BC planning: Are all your bases covered?.......... 6
The costs of downtime 7
Failing to plan is planning to fail........................ 7

BC planning defined.. 8
The evolution of BC planning: a brief history..... 9
Why you should implement BC planning now... 10
BC regulations and standards........................... 11
Getting top management buy in....................... 12

BC planning methodology................................ 13
Assemble the team.. 13
The five phases of implementation.................... 14
Phase 1: Identify
Phase 2: Analyze
Phase 3: Design
Phase 4: Plan development and execution
Phase 5: Test and maintenance
Getting started: risk assessment........................ 15
Threat factors, probability and impact on functional areas.. 17
Risk analysis matrix.. 18

Some BC best practices.................................. 19

Summary.. 20

BC planning: are all your bases covered?

Over the past 30 years, business continuity planning, or BC planning, has evolved from something a few companies in highly regulated industries—such as the financial sector—had to do, to becoming recognized as an imperative for every company and government entity, large or small. BC planning is the answer to the question, "What if…?" and can easily spell the difference between the continued operation or permanent shut down of your organization should a disaster occur.

If you think it can't happen to you, consider these plausible scenarios:

- Your company's network goes down for nearly a day. You can't service your customers, who start calling your competitors. What do you do?
- Your website, which is your company's storefront, is down. Orders are lost; customers lose access to services on your site. How long can you afford to stay down?
- Days of heavy rain and severe flooding wash out roads and block access to your facility. Employees can't come to work. How will this affect your business?
- The local power company has a failure in your area. Power is out for hours. Your offices are dark, your manufacturing floor idle. What do you do?
- A hacker gets into your system, hijacks your customer database, and steals the identities of your customers. How will you repair the damage?
- A disgruntled employee steals intellectual property from your network and exposes it to your competitors. How will you overcome this exposure?
- Your business is located on the same street as the courthouse. A controversial case is being tried, resulting in violent street protests outside your building. How will you safe-guard your employees and maintain operations?
- Careless construction workers on your street cut the fiber optic connection to your facility, severing your phone and Internet access. Service will not be restored for hours, if not days. What now?
- A powerful earthquake strikes in the middle of the day. There is structural damage to your facility. Some employees are unaccounted for. What actions will you take?
- A flu epidemic has broken out in your city. Its symptoms are debilitating, and if left untreated, can actually result in death. What precautions can you take, and how will you maintain operations if the epidemic causes mass absenteeism?
- Several of your top executives are tragically lost in an airline accident. How will your organization handle the short- and long-term implications?
- In a very rare occurrence, a volcano erupts in Iceland, spewing ash across Europe and grinding air transport to a halt. Many of your key executives are grounded, and shipments to your factories are stalled. What plans do you have in place to mitigate the loss?
- One of your offshore oil rigs has exploded. Lives have been lost, and oil is spewing into the ocean at the rate of thousands of barrels per day. How will you stop the spillage; mitigate the contamination of the environment; compensate people and businesses whose livelihoods were severely impacted by the spill; manage the massive negative press; handle the slew of lawsuits that will be filed against your company; deal with the criminal charges which will be filed against your top executives for gross negligence; and answer to the U.S. government and the American people for what is being called the worst environmental disaster in U.S. history?

Perhaps the most dramatic and illustrative case for BC planning is the attacks on the World Trade Center. In the first attacks in 1993, terrorists set off explosives, which caused fires to rage in the complex. As many as 44% of the businesses housed in the buildings ceased operations at least temporarily, and 150 out of the 350 business affected closed their doors for good.

After this, many companies with offices in the World Trade Center implemented business continuity plans. When terrorists brought down the twin towers on September 11, 2001, while many companies again permanently ceased operations, those companies that had comprehensive continuity plans in place were up and running again in just days.

The costs of downtime.

The American Management Association has stated that, "About 50% of businesses that suffer from a major disaster without a disaster recovery plan in place never re-open for business." But even minor disasters can be devastating. One study by a business continuity group revealed that 54% of businesses surveyed estimated that an hour of downtime would cost them anywhere from $51,000 to $1 million. A similar survey found that the average time to restore availability of critical information systems was nine to 12 hours. Without mitigation plans in place, such costs could quickly add up and cripple or shut down a business. And a report from a major CPA and auditing firm reveals that if a company loses access to core data for two weeks, it will take up to nine months to make up the loss in revenue caused by that two-week breach. Most firms can't survive such a scenario.

A well-known industry analyst organization outlines the potential costs of downtime this way:

- **Productivity**
  - Number of employees affected, multiplied by hours out, again multiplied by hourly rate
- **Revenue**
  - Direct loss
  - Compensatory payments
  - Lost future revenue
  - Billing losses
  - Investment losses
- **Financial Performance**
  - Revenue recognition
  - Cash flow
  - Lost discounts (A/P)
  - Payment guarantees
  - Credit rating
  - Stock price
- **Damaged Reputation**
  - Customers, suppliers, financial markets, banks, business partners
- **Other expenses**
  - Temporary employees, equipment rental, overtime costs, extra shipping costs, travel expenses, legal obligations

Failing to plan is planning to fail

When it comes to business interruptions, it is not a matter of if, but of when, how, and how severe; and in relation to this, no adage has ever been truer: failing to plan is planning to fail. It is critical that you not only implement a business continuity plan, but that you make sure you truly have all bases covered. To that end, this chapter will give you a review of BC planning, including:

- BC planning defined
- The evolution of BC planning
- Why you should implement a BC plan now
- Regulations and standards
- Getting top management buy-in
- The methodology of formulating and implementing your plan
- Getting started: risk assessment
- Some BC best practices

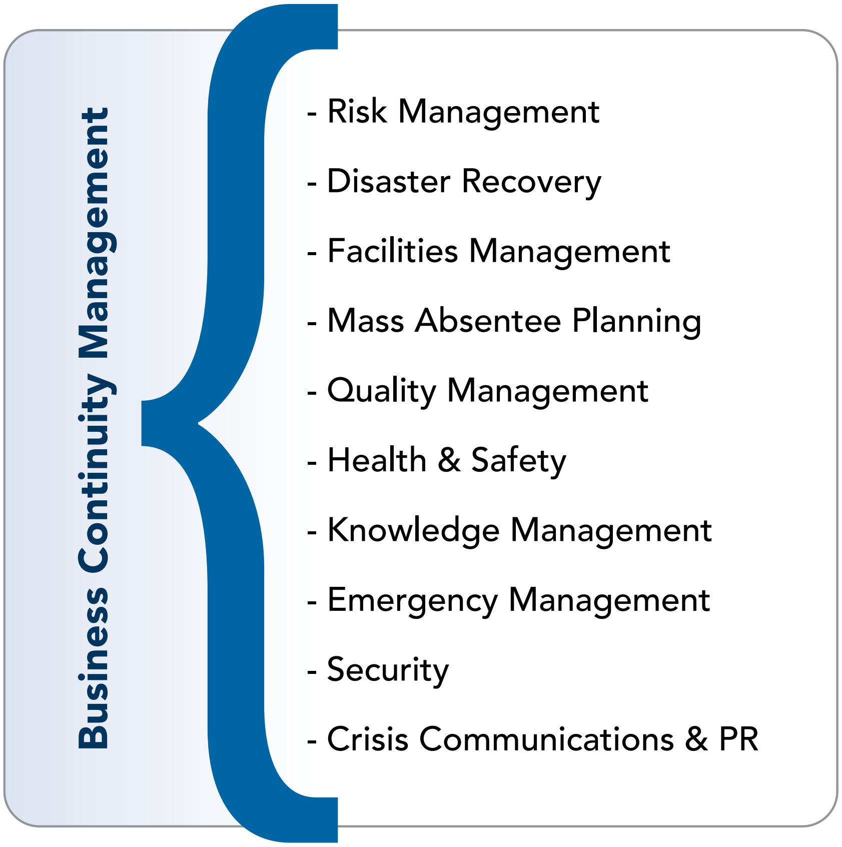
BC planning defined

Put simply, BC planning is the continuous process of identifying risks and their impact on critical business functions in your organization, and developing strategies and procedures for 1) mitigating risks; and 2) restoring functions as quickly as possible when a disruptive event occurs.

You'll often see the term BC/DR, which stands for business continuity/disaster recovery. They are not the same. Disaster recovery is actually a subset of business continuity. Here are the differences:

- **Business continuity planning:** An all-encompassing approach whereby organizations plan for recovery of the entire business process. This includes a plan for human resources, facilities, workspaces, documentation, supply chain and technology
- **Disaster recovery:** A technology-driven approach where procedures have been implemented to ensure the effective maintenance of critical IT systems, applications, and data

In the early days of business continuity, planning focused primarily on disaster recovery. Over the past thirty years, and particularly after 9/11, BC planning has necessarily evolved to take a holistic view of all business processes.



Business Continuity Management

- Risk Management
- Disaster Recovery
- Facilities Management
- Mass Absentee Planning
- Quality Management
- Health & Safety
- Knowledge Management
- Emergency Management
- Security
- Crisis Communications & PR

The evolution of BC planning: a brief history

While BC planning as a formally-recognized discipline has only been around since the late 1970s, the concept of BC planning is actually quite ancient. In fact, Sun Tzu, one of the most influential military strategists of all time, wrote about contingency thinking some 2,600 years ago, highlighting the need for backups (weapons caches) and scenario planning to foresee and prepare for possible events.

> While BC planning as a formally recognized discipline has only been around since the late 1970s, the concept of BC planning is actually quite ancient.

The 1970s – 1990s
Fast forward to recent times. In the early 1970s, Pierre Wack, a planner in the London office of Royal Dutch Shell and a pioneer of scenario-based planning in business, used it to good effect for his company. Wack accurately predicted that OPEC would disrupt the oil market by demanding high prices for oil—which it did after the 1973 Yom Kippur War in the Middle East. Shell was one of the few oil companies prepared for this contingency, allowing it to move from being one of the weaker oil companies to one of the strongest and most profitable. Shell's planning group subsequently foresaw the possibility of losing access to critical oil pricing and sales data housed on its mainframes. This led to the company investing in IT backups. In fact, Shell was the first commercial user of an offsite storage facility, trusting its data assets to the original Iron Mountain. This marked the birth of the BC/DR market as we know it.

Also during the 1970s, another oil giant, Sun Company, formed a subsidiary named SunGard (now one of the biggest names in the business continuity industry) to provide remote-access data processing for Sun's information Services (SIS). By the late 1970s, Sun had become so reliant on its computer systems that a computer failure could result in losses in the millions of dollars. This led SIS to implement daily backups to tape stored off-site which could be loaded to an alternate mainframe should Sun's primary mainframe fail. In 1978, a group of Philadelphia businesses seeking a similar disaster recovery solution approached Sun, leading to SunGard Recovery Services becoming a commercial hot-site provider.

This was the beginning of a new industry. By 1979, there were over 100 such providers across the U.S., and during the 1990s, the hot-site, alternate computer center industry grew to over $620 million in annual subscription fees, with most customers served by three companies: IBM, SunGard and Comdisco. During this time, BC was primarily focused on disaster recovery—that is, in the event of a disaster, an organization's technology assets (networks, applications and data) would be recovered at an alternate location, with a typical recovery time objective (RTO), or time to recover operations, of 24 hours.

Most of the companies that implemented disaster recovery plans were in highly-regulated industries such as banking and other financial sectors (the original Federal Financial Examination Council BCP Handbook was published at this time). There was also a growing awareness of the need to expand business continuity to include all business processes, not just technology. This progressed slowly at first, but accelerated as enterprises made preparations for the potential Year 2000 (Y2K) crisis. As they prepared their Y2K contingency plans, many enterprises realized that if their critical systems and applications failed, so would their business processes. This hastened investment in BC/DR, with both reduced RTO for mission critical operations and recovery point objectives (RPOs), or lag time in restoring data, set to the point the disaster occurred (meaning, no loss of data). Another key trend influencing this growth in BC/DR was the recent explosive growth in Internet-based business and reliance on constant uptime to maintain steady operations with customers, suppliers and business partners.

Then Y2K came and went and turned out to be largely uneventful. Enterprise and government breathed a collective sigh of relief. All was good—until the terrorist attacks of September 11, 2001.

September 11, 2001: The day that changed everything.

The events of 9/11 disrupted continuity on an unprecedented scale. Entire workforces were wiped out, including key executives, IT organizations and disaster recovery teams that could have otherwise implemented BC/DR for their firms. There was complete destruction of physical facilities and unrecoverable loss of records, systems and other enterprise assets. Communications were cut. Transportation was hampered, with air transport completely halted. Mail and courier services were delayed. After 9/11 there was a collective awareness of the urgency of having comprehensive, tested business continuity plans for all organizations to ensure their very survival.

2002 – today

It is surprising then, that even with the wake-up call of 9/11, and subsequently the tsunami in Indonesia in 2004, Hurricane Katrina in 2005, and numerous other disasters in recent years, BC/DR planners continued to struggle with corporate apathy and lack of support from top executives. Perhaps BC/DR was viewed as an optional insurance plan against unlikely events, was perceived as too costly and complex to implement, or a combination of these. This has spawned a new industry of hardware and software providers and consulting firms helping to demystify and ease the implementation of BC/DR, and spurred the growth of industry associations, certification bodies and business school programs focusing specifically on BC/DR. The previous decade has also seen the publication of a whole new crop of industry-specific statutes, regulations and standards, with legal implications for non-compliance (see Regulations and Standards later in this chapter). Indeed, BC/DR has become very serious business, as well it should be.

Why you should implement BC planning now

The most important reasons to implement a BC plan in your organization as soon and as thoroughly as possible are:

- It will save lives when—not if—a disaster strikes
- The survival of your business will depend on it; it's only a matter of time
- It meets your obligation to your stakeholders, shareholders and customers to exercise a minimum standard of care and preparedness
- In many cases, it is the law, and without a BC plan, your top executives and your corporation could face criminal charges, heavy fines, and even jail time
- It's good business. BC planning will help you maintain service to your customers, protect employees and assets, and minimize financial losses

Making BC a way of life will allow your organization to consistently:

- Identify and mitigate risks before a disaster occurs
- Minimize decision-making time during a disaster
- Instill a culture of calm preparedness and action for whenever a drastic event occurs
- Provide for an orderly and expedited recovery after a disaster
- Ensure organizational stability
- Reduce reliance on only a few key personnel
- Reduce potential legal liability
- Preserve the ability to meet your customers' expectations in a wide range of circumstances, including meeting your service level agreements
- Safeguard your company's reputation and brand
- Maintain or gain competitive advantage due to a swift and effective response

- Gain early warning of and take corrective action on any weaknesses or vulnerabilities in your business
- Potentially realize improvements in your insurance costs and coverage

BC regulations and standards

Many regulations and standards have been published since the 1990s covering numerous industries. Understanding those that pertain to your organization isn't just good practice—failure to comply could result in harm to your employees, irreparable damage to your business, and legal action if events are not handled properly.

Following is a partial list of the regulations, standards and guidelines from the past two decades. Many are available on the Internet while others can be purchased from the standards bodies and associations that publish them.

- **FFIEC BCP Handbook** – Federal Financial Institutions Examination Council guidelines. A comprehensive standard to follow for any organization
- **NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs** – General facility safety and resilience guidelines published by the National Fire Protection Association
- **Australian Standards BCM Handbook**
- **Basel Capital Accord** – Basel Committee on Banking Supervision guidelines for assessing credit and operational risks for banks
- **MAS BCP Guidelines** – Business continuity management guidelines published by the Monetary Authority of Singapore
- **FSA Handbook** – Published by the Financial Services Authority in the UK for insurers, investment firms, mortgage firms, banks and other financial firms
- **Civil Contingencies Act** – An act of the Parliament of the UK providing a framework for emergency planning and response from the local to the national level
- **ISO 22301** was built on the foundation provided by BS 25999-2 and uses that best-practice approach at its basis.
- **Health Insurance Portability and Accountability Act (HIPAA) of 1996** – BC regulations for the healthcare industry
- **Sarbanes-Oxley Act of 2002 (SOX)** – Major changes to regulation of financial practice and corporate governance after 9/11 and the Enron scandal
- **NASD Rule 3500 Series** – NASD, now known as Financial Industry Regulatory Authority (FINRA), created these SEC approved rules for BC planning
- **NYSE Rule 446** – SEC approved rule for BC in the financial sector
- **NERC Security Guidelines** – Cyber-security rules from the N. American Electric Reliability Council
- **FERC Security Standards** – Cyber-security rules from the Federal Energy Regulatory Commission
- **NAIC Standard on BCP** – Published by the National Association of Insurance Commissioners
- **9/11 Commission Final Report**
- **NIST Contingency Planning Guide for Information Technology Systems** – Recommendations of the National Institute of Standards and Technology
- **FRB-OCC-SEC Guidelines** – *Interagency White Paper on Sound Practices to Strengthen the US Financial System* published by the Federal Reserve Board, Office of the comptroller of the Currency and the Securities and Exchange Commission
- **Fair Credit Reporting Act** – Amended by the USA Patriot Act of 2001 and the Fair and Accurate Credit Transactions Act of 2003 to protect data integrity; ensures accuracy of credit reporting
- **California SB 1386** – Regulates the privacy of personal information
- **GAO Potential Terrorist Attacks Guideline** – 2003 report to Congress by the US General Accounting Office on additional actions needed to prepare critical financial market participants

- **Federal Legislative BC Requirements for IRS** – Includes protection of company records
- **NFA Compliance Rule 2-38** – National Futures Association compliance rules for BC/DR planning
- **NY State Insurance Circular Letter No. 7** – Disaster planning and preparedness response for life insurers and property/casualty insurance industries in New York
- **ASIS International Organizational Resilience, ANSI Standard** – Organization resilience best practices published by the International Association for Security Professionals
- **National Institute of Standards and Technology (NIST)** – Best practices for information security
- **NISCC Good Practice Guide to Telecommunications Resilience** – The UK government's National Infrastructure Security Coordination Centre's recommendations for telecommunications resilience in organizations
- **Federal Information Security Management Act of 2002** – Requires federal government agency program officials, CIOs and inspectors general to conduct annual information security program reviews
- **Patriot Act** – This anti-terrorism act includes record retention requirements to comply with its Customer Identification Program
- **ISO 27001** – Guidelines for information security management in an organization

Note that if you are a supplier to a customer who is in one of the industries covered by regulations and standards, you may be held to those same standards. For instance, if you are a paper document manufacturer or data warehousing facility serving customers in the banking industry, then you'll be required by your customers to build a BC plan that meets the FFIEC requirements, as well as Sarbanes-Oxley requirements, such as having client data going back at least seven years available at all times. In other words, if your customer is regulated, so are you, and if you fail to have an adequate BC plan then you'll lose that customer.

Getting top management buy-in

When it comes to implementing BC, it is simply not in the nature of organizations for support to come from below. Staff has too many other departmental duties and deliverables on their plates to make organizational BC/DR a priority. To gain participation across the organization, BC has to be mandated from the top. But even today, gaining the attention of top management, much less buy in and active support, is an uphill battle for BC/DR planners, many of whom themselves have other departmental duties of their own.

To get the support you need for your effort, here is a list of tips for gaining top management buy-in:

1. **Go in with specific objectives** – Know exactly how much funding is needed and what level of support you need from top management and the organization.
2. **Take what you can get** – If your proposal calls for a two-hour RPO and management is willing to commit to achieving a 24-hour RPO, take the 24-hour RPO over outright rejection.
3. **Be ready to overcome objections** – For instance, if the objection is cost, be prepared to justify the effort as an investment.
4. **Present the benefits** – Benefits can include the safeguarding of people, assets, data, reputation and customer relationships, and avoiding the costs of downtime.
5. **Make the ROI case** – Show not only how much business and revenue can be salvaged with BC planning, but also how daily operations and competitiveness are improved.
6. **Research the competition** – If your top competitors are investing in BC, your management will be more likely to buy-in.
7. **Recruit others in the organization to back you up** – If you already have the support of staff in other departments, you'll have an easier time selling executive management.
8. **Scare them with the legal ramifications** – After a major disaster, every communication and action taken by top management before,

during and after the event will be highly scrutinized and second-guessed by regulators. Did the company adhere to statutes, industry regulations and standards for having and implementing a proper BC plan? Prosecutors may also use the "Prudent Man" standard, derived from common law, to establish if your management exercised a minimum standard of care to safeguard life and assets as compared to the actions of a reasonable person in similar circumstances. In fact, your management may be held to a higher standard of care, as arguably, they are more knowledgeable and skilled than an ordinary person. Ultimately, they may be found criminally liable and face heavy fines, jail time or both. On top of this, employees, investors, customers and other stakeholders may sue management and the organization itself with the potential for damages in the millions or even billions of dollars.

> Your team should include expertise in all the business processes and technical aspects of your organization, of which many or all will come into play during an event.

BC planning methodology

Assemble the team

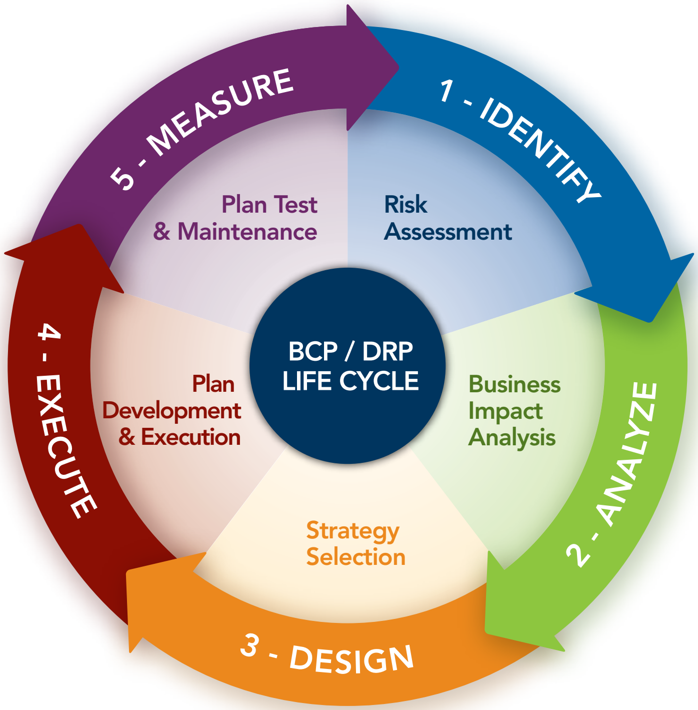
Once you've obtained top management buy-in, including budget approval, you'll next need to create your BC implementation team. The makeup and size of this team will vary depending on the type and size of the organization. A typical team will include:

- A senior representative from top management to champion the initiative and to keep the implementation process a high priority throughout the organization
- A BC coordinator reporting directly to the senior representative who will manage the process and lead the team. You may consider having two coordinators, one representing business processes, the other representing technical aspects (IT, backup, telecommunications, etc)
- Additional BC analysts, lower-level teams and administrative staff appropriate for your size and type of organization
- If your organization is larger, matrix team management will be the most effective approach. The team will consist of existing managers from key divisions, departments and locations. While BC planning won't be a full-time project for them, they will be expected to devote appropriate time to the process

Your team should include expertise and functional responsibility in all the business processes and technical aspects of your organization, of which many or all will come into play during an event:

- Damage assessment and recovery
- Facilities and security
- Logistics and transportation
- Supply chain and procurement
- IT
- Telecommunications
- Accounting
- HR
- PR/communications
- Marketing, sales and customer service
- Legal counsel

The five phases of implementation



With your team assembled, it's time to apply a methodology for implementing a BC plan in five distinct phases. Keep in mind that because your organization's internal and external operating environments are always changing, BC planning is an ongoing and cyclical process.

Phase 1: Identify

In this phase, you'll conduct a risk assessment, identifying any potential hazards that could disrupt your business and the likelihood and severity of impact on your organization. The next section of this guide goes into more detail about this phase.

Phase 2: Analyze

Next, you'll perform a business impact analysis (BIA). The BIA identifies key business functions and the financial and non-financial impact on the organization of interruptions to those functions for any length of time. For each business function, the BIA specifies:

- Recovery time objective (RTO) – the acceptable amount of time to recover the function
- Recovery point objective (RPO) – the acceptable lag in data concurrency from the time of the interruption (an RPO of zero would mean data must be restored to exactly as it was at the time of interruption with no data loss)
- Minimum operating resources
- Internal and external dependencies

The BIA is essentially the foundation of the BC plan. Without a well-researched and formulated BIA, the BC plan will be likely be flawed. For this reason, the entire second chapter in *The Definitive Guide to Business Continuity Planning* is devoted to the BIA.

Phase 3: Design

In this phase you'll develop mitigation and recovery strategies to protect your people, assets and business functions, including employee safety, network failover, manual and technical procedures, alternate worksites, staffing issues, vendor issues and crisis communication. The third chapter in this guide describes this phase in full detail.

Phase 4: Plan development and execution

With your strategies formulated, it's time to detail them in a concise, well organized and easy-to-follow document or set of documents. Your plan will include an executive summary, employee safety, recovery procedures, incident response, command and control, crisis communications and business resumption. You may choose to follow industry-specific templates for documenting your plan, or create a format tailored to your specific needs. Then you'll publish the plan, disseminate it to staff and train your staff on how to use it (execution). Plan development is detailed in the third chapter in this guide, and execution is fully described in the fifth chapter.

Tools

There are a variety of tools available to help you organize, document and implement your plan, including Microsoft Office, Visio, BC planning software, risk assessment and management tools, crisis management tools and mass notification tools. The fourth chapter in the guide will help you better understand the pros and cons of the available tools and how to make the best use of them.

Phase 5: Test and maintenance

A plan isn't truly a plan until it has been thoroughly tested. Tests take many forms, including company testing, examination scrutiny, and audits, both internal and external.

Testing

- Company testing: Take your staff through real-life scenarios, including actual role-playing, to test how easily the plan documentation is understood, how easy it is to implement, and if it has all the information required to appropriately deal with each situation. Testing will not only verify strategy, but also expose gaps
- Examination scrutiny and audits: Does your BC plan adhere to all applicable statutes, regulations and standards?

Maintenance

- At the conclusion of testing you'll make changes to the plan to correct any uncovered deficiencies. At this point, the cycle is complete and begins again. Periodically reassess risks, impacts and strategies, make corrections as necessary, and retest frequently to ensure the most effective plan
- The fifth and final chapter in the guide covers test and maintenance in full detail

Getting started: risk assessment

Risk Assessment is the important first phase of creating your BC plan. Think about every conceivable threat to your business processes, large or small, likely or rare. Threats can be broken down into three categories: natural threats, human threats and technical threats. Examples of threats in each category follow. Perhaps you can think of more that are directly applicable to your organization's environment.

Threat types

Natural Threats

- Hurricane/tropical storm
- Internal flooding (pipe burst, overflow, etc.)
- External flooding (river, dam, flood plain, etc.)
- Internal or external fire
- Seismic damage
- Wind damage
- Tornado
- Aircraft incident (on-site helipad, nearby airport flight path, etc.)
- Severe winter weather (extreme cold, extreme snowfall, ice storm, etc.)

Human Threats

- Explosion (gas, steam, etc.)
- Executive management lost in common accident
- Extortion
- Burglary

- Embezzlement
- Transit disruption (strike)
- Vandalism
- Riot/civil unrest
- Robbery
- Domestic/corporate terrorism or sabotage
- International terrorism (due to proximity of target organizations – military base, foreign embassy, major attraction, etc.)
- Nuclear accident – direct impact (evacuation required)
- Nuclear fallout – indirect impact (evacuation may be required)
- Influenza outbreak
- Hazardous material/waste – in transit
- Workplace violence
- Labor dispute or strike
- Work stoppage
- Data entry error
- Improper handling of sensitive data
- Unauthorized physical access
- Malicious damage or destruction of software or data
- Unauthorized physical access
- Unauthorized access to data
- Theft of data
- Unauthorized modification of software or hardware

Technical Threats

- Power – fluctuations and failure
- Heating, ventilation or air conditioning failure (HVAC)
- Malfunction or failure of computer servers or hardware
- Failure of system software
- Failure of application software
- Data network loss
- Telephone service loss
- ISP – Internet access loss
- Electromagnetic interference

Threat factors, probability and impact on functional areas

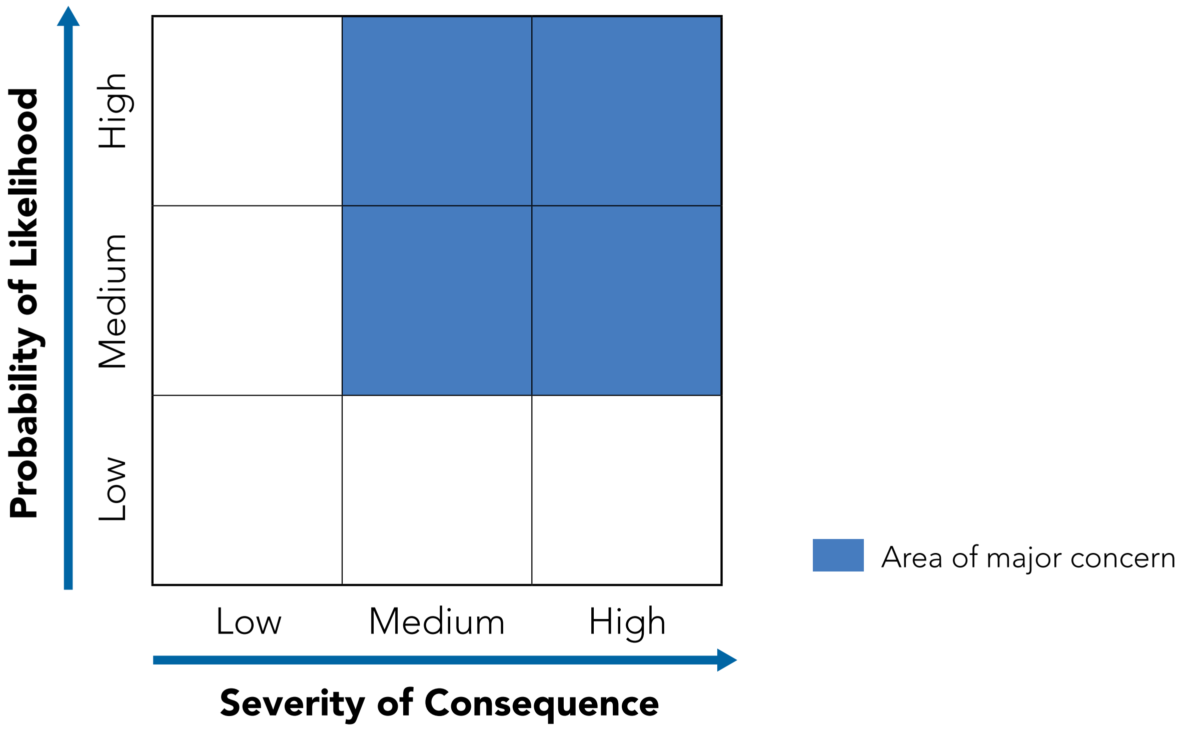
Once you've identified all potential threats, you'll want to rate each one according to the following criteria, with point values for each, to arrive at a weighted score for each potential threat:

- **Speed of onset:** sudden or gradual
- **Forewarning:** yes or no
- **Duration:** long, medium or short
- **Probability:** high, medium or low
- **Impact on functional areas:** 0, 1, 2, or 3 (highest impact)

RISK FACTOR	RATING CRITERIA			TOTAL SCORE	COMMENTS
Description	**Event likelihood** 0 - No Risk 1 - Minimal Risk 2 - Significant Risk 3 - Prevalent Risk	**Anticipated impact on organization** 0 - No Disruption 1 - Minor Disruption 2 - Moderate Disruption 3 - Full Disruption	**Anticipated duration of disturbance** 0 - Minimal (Momentary) 1 - Up to 1 Day 2 - Up to 1 Week 3 - More than 1 Week		Basis for Assigned Ratings
NATURAL ENVIRONMENTAL THREATS					
Hurricane/Tropical Storm	1	1	1	3	Periodic hurricane remnants can impact area for approximately one day.
Internal Flooding (Pipe Burst, Overflow, etc)	3	2	2	**7**	Building has history of flooring incidents; Unprotected sprinkler in server room.
External Flooding (River, Dam, Flood Plain, etc)	1	2	2	5	No prevalent risk observed, but communications room in basement would be disrupted if a flood did occur.
Seismic Damage - Earthquake	0	0	0	0	No significant threat identified.
Wind Damage	1	0	0	1	Very slight potential of occurence but minimal impact expected.
Electrical Storm	1	1	1	3	Relatively frequent occurence with potential for power outage or other damage.
Tornado	1	2	2	5	Infrequent occurence but potential for damage is substantial.
Severe Winter Weather (Large Snowfall, Extreme Cold, Ice, etc)	1	1	1	3	Could inhibit employees' ability to report for work.
Internal Fire	1	3	2	**6**	Multiple restaurants located in building.
External Fire	1	0	0	1	Building is disconnected from other buildings except by a parking garage.

With all threats identified (or at least as many as your team can possibly think of), and scores assigned to each one, you can systematically prioritize threats by likelihood, timing and impact and start to determine the appropriate response to each. This is essential to guiding your BC/DR planning efforts and finite resources to where they'll likely be needed the most.

Risk analysis matrix



The next step is to complete your business impact analysis (BIA), which is covered in the second chapter.

Some BC best practices

As you and your team begin to embrace the significant task of creating your organization's BC plan, it will be helpful to know some key best practices before you get started. Consider the following lessons learned over the years.

- **Don't cut corners**
  - **Business continuity is a process, not a checklist.** There are no shortcuts to properly assessing risk and impacts, developing proper mitigation strategies, implementing your program organization-wide and testing it for efficacy
  - **Business continuity is a continuous program, not a one-off project.** You must continually exercise and evaluate your plan to keep it current, viable and focused on the right priorities
  - **Perform a thorough risk analysis and BIA.** Do your homework, perform thorough data gathering and analysis, and consider as many potential risks and scenarios as possible. Many companies cut corners with these steps. Trying to write plans without doing your homework is like building a house with no foundation. Your plan will not reflect actual risks and their impacts to your critical business processes and will not stand up to actual disruptive events; i.e., your house will come crumbling down

- **Keep it simple**
  - **Don't try to do it all at once.** Implementing a BC plan is a culture shift for any company, so be prepared for a lengthy process. Breaking down your rollout plan into smaller projects will help you better manage all the details and prioritize elements of the deployment
  - **Don't create the perfect plan.** Invariably, it will be obsolete by the time you publish it. Circumstances and personnel are constantly changing
  - **Don't produce a 100-page document.** Nobody will read it, especially in a time of crisis. Make it short and easy to refer to in a hurry
  - **Avoid BC jargon.** Most people won't understand buzzwords. Make it easy to understand

- **Don't try to cater to every conceivable scenario**
  - Create classes of scenarios with good basics for handling most situations

- **Stretch your BC planning budget**
  - Defray costs by using current assets such as other office and co-location facilities
  - Work with your IT department to tie the IT management budget to BC to provide not just resiliency in the face of disaster, but also high availability for daily operations

- **Don't reinvent the wheel**
  - **Learn from past experiences.** There is a wealth of information on the Internet, among your industry colleagues, and within your own organization
  - **Follow a standard or handbook.** FFIEC BCP Handbook (U.S., Financial), NFPA 1600 (U.S., all organization types), ISO 22301 (based on BS25999), HB292/293 (Australia) are just a few of the thorough tools that are available to you
  - **Use technology.** There are excellent BC software tools on the market that can integrate data from your company's various personnel and CRM databases, and organize your various planning documents so you can avoid duplicating data and having to rely on bloated Word documents. You can also store plans on mobile devices to empower your workforce. From a resiliency standpoint, use of cloud computing resources (everything from BC software to automated, emergency mass notification and response systems), storage virtualization and hot-sites can remove single points of failure and help keep your business running with minimal interruption

- **Plan exercises at convenient times**
  - For instance, plan an exercise when your IT department is doing scheduled maintenance anyway. Work-from-home pandemic scenarios may also prove popular

- **Practice frequently**
  - Start with simple plan reviews
  - Then try smaller, manageable areas before

1
2
3
4
5

going to full-scale, organization-wide exercises

- Involve people in your organization who've previously experienced disruptions and disasters—they'll be great ambassadors and sources of useful information
- Use scenarios that are meaningful and credible to your employees, and if possible, include scenarios they've already experienced
- Practice at least two or three times per year and consider monthly exercises to maintain facility with your plan and provide more opportunities to expose and correct gaps
- Consistent, frequent practice will build confidence in your BC team and across the organization

- **Involve your stakeholders at every step**.
  - Allow them to have input to and ownership of the plan, especially the parts that pertain directly to their departments and functions. You'll get much better participation and more effective implementation
- **Review your plan whenever there is a change in your organization that may affect the plan**
  - that can include anything from a software update on a critical server to a member of the BC team leaving the company
- **Make BC part of your everyday culture.**
  - If BC is something your staff has top-of-mind every day, they'll be ahead of the game when an actual event occurs. Daily or weekly email reminders, signage around the facility, and an internal BC Web portal are all good ways to achieve this

Summary

Having your BC bases covered means understanding what BC planning is, how it's evolved, why it's so important to your organization, which regulations and standards you must adhere to, how to get top management buy in, what are the five essential phases, why you must start your BC planning process with a thorough risk assessment and what are the best practices for getting it done.

Now that you've reviewed the essentials of BC planning and considered your risk assessment, it's time to begin your business impact analysis (BIA), the subject of the next chapter.

CHAPTER 2

Business Impact Analysis: The all-important foundation

Business Impact Analysis: The all-important foundation

CHAPTER 2

Situation

You've committed to developing a BC plan to protect your organization and have performed a thorough risk analysis. The next step is to perform a business impact analysis, or BIA. The BIA helps you understand the impact disruptions would have on your business: which processes would be disrupted, how severe the impact would be, and how long your business could survive without those processes running.

Need

When an event happens, you'll have little or no time to assess which affected business processes are most vital at that point in time. You'll need to make crucial decisions quickly to divert resources to maintain operations while recovering disrupted processes. Without a BIA in place, you'll have to guess what to do in those first few critical minutes and hope you've made the right decisions. Make the wrong decisions and there could be a chain of disastrous results, from organizational failure, to lawsuits, prosecution and even loss of life. Preparing a BIA guides you in prioritizing processes and the resources they depend on, and takes the guesswork out of decision-making in a crisis.

Challenge

There are no shortcuts to creating a good BIA. You must invest time and resources to identify and analyze your processes to prioritize resources and strategies for their recovery. To keep your BIA up to date you'll have to regularly reevaluate and update it, making BC planning an integral part of your company's culture.

Solution

This chapter will guide you through a step-by-step methodology for building a BIA, including getting top management buy-in, helping your organization take ownership, gathering necessary data, identifying your processes, prioritizing their importance and seeing how they depend upon each other to function properly. It will guide you in creating a BIA to meet your organization's needs while being simple enough for everyone to use.

Results

By understanding both the risk of disruptive events occurring (risk assessment), the impact they'll have on your processes, which processes require attention first, and what resources are necessary for recovery, you'll have the information you need to create effective recovery strategies to protect your business, whatever may happen.

What exactly is a business impact analysis (BIA)?.. 23

Why you must do a BIA...................................... 23
Eliminate guesswork when disaster strikes......... 23
Allocate your resources in a crisis........................ 24
Create solid test criteria for your plans and suppliers.. 24

Prerequisites for a successful BIA...................... 25
Get senior management buy-in.......................... 25
Make it part of the culture.................................. 25
Keep it simple.. 25
Consider having a professional lead the BIA process... 25

Data gathering... 26
What data?... 26
Data gathering methods...................................... 26

Impact assessment.. 27
Assess impact, not causation............................... 27
Impact scenarios.. 27
Impact categories... 27
Impact severity... 28
Interdependencies.. 28

Recovery requirements....................................... 28
RTO: recovery time objective.............................. 28
RPO: recovery point objective............................. 29
Recovery resources.. 29

Completing a BIA matrix..................................... 30

Finalize your BIA.. 30

Summary.. 30

What exactly is a business impact analysis (BIA)?

As its name suggests, the business impact analysis, or BIA as it's commonly known, is a thorough, methodical process for analyzing the impact of interruptions on your daily operations. By performing a BIA you will:

- Identify all of your business functions, from the organization-wide level to division and department levels
- Understand how critical each process is to the healthy operation of your organization
- See the dependencies critical processes have on other processes and resources, which themselves become critical
- Understand the type and severity of impact a disruption to any process can have on your organization, including financial, operational, legal, on your customers and to your reputation
- Gauge the maximum amount of time your organization can go without any given process before its health and even survival become jeopardized (maximum allowable downtime or "MAD")
- Understand the resources required to recover processes to a minimum acceptable level within the maximum allowable downtime window
- Prioritize the allocation of recovery activities and resources in advance of a potential disruption to restore the most critical processes first when a disruption occurs
- Create a sound recovery strategy (covered in the third chapter of *The Definitive Guide to Business Continuity Planning*)

In short, the process of conducting a BIA is priority-setting—identifying those processes that are most vital, understanding how long you can go without those processes, and prioritizing resources to keep those vital processes running at minimum levels while restoring them to full health as quickly as possible should a disruption occur.

Why you must do a BIA

1. Eliminate guesswork when disaster strikes

Plain and simple, there's no way to create an effective recovery strategy without an accurate and current BIA. Not having a BIA is like having a life-threatening accident and seeing a trauma physician who has no idea which bodily functions are most critical to your survival, nor how best to restore those functions before you succumb. All he or she can do is guess how to fix you. Like that physician, you'll be guessing what to do when a disruption to your business occurs.

Conversely, a knowledgeable physician will quickly assess what's wrong with you and employ the proper procedures to stabilize you. You want to be like that knowledgeable physician—knowing exactly what your organization's vital functions are—i.e., how long the patient can go with a lack of oxygen, body temperature and blood pressure at unstable levels, inadequate blood supply, etc.—and how to restore those vital functions to minimum safe levels to avert a catastrophic result. The physician looks at you systemically, which is precisely what the BC professional needs to do. That's why physicians train for years before going into practice—to minimize guesswork when they treat a patient. Likewise, a BIA will take the guesswork out of planning how to recover your business.

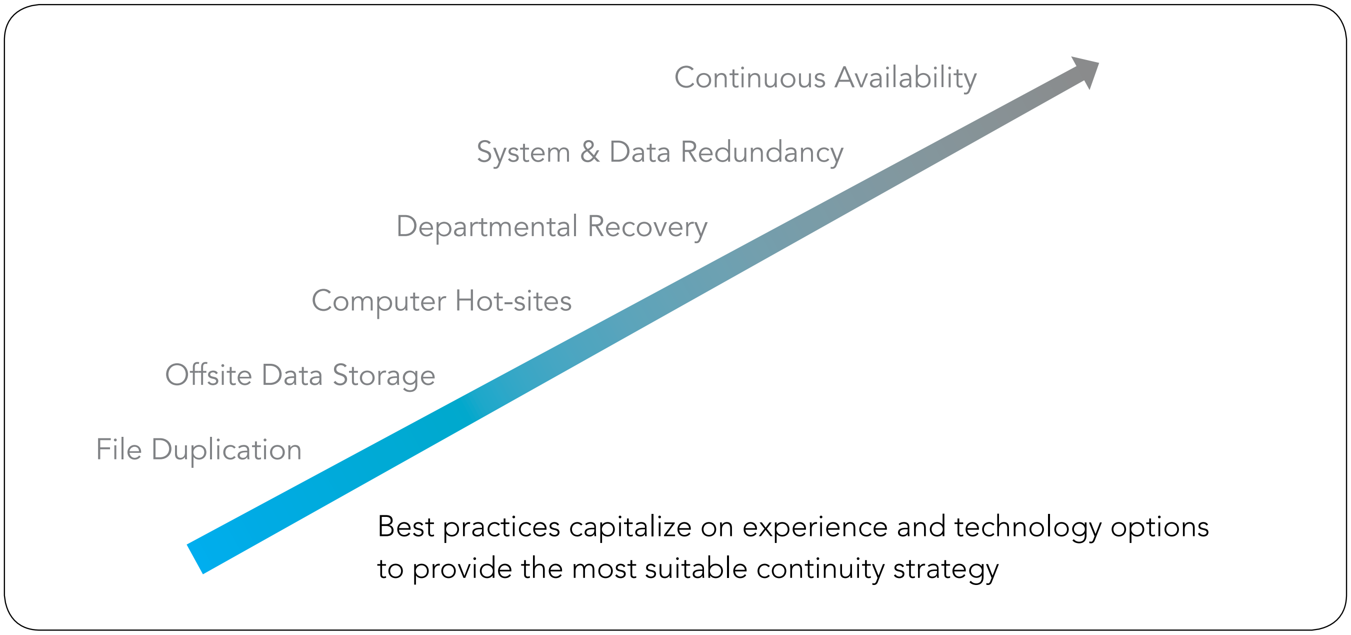
Physicians have a minimum standard of care. So do you. Without a BIA, your decisions in times of crisis will be arbitrary. You'll have no way to justify the actions you took, or didn't take, after the fact. With a solid BIA, you'll have the justification you need for the decisions you and your management will make, based on solid, comprehensive data and sound analysis. In other words, you've done your due diligence. And the good news is, it won't take you years of training to do the BIA. Quite the opposite—you can prepare a solid BIA in a matter of weeks. This chapter will help get you started.

2. Allocate your resources in a crisis

We all have limited resources. Your organization can't afford to lavish money, technology and people on preparing for every contingency and ensuring near-total uptime for every process. You must carefully allocate limited resources where they'll be needed most. Again, having a BIA takes the guesswork out of that. With a well-crafted BIA, you'll know in advance which processes are critical to your survival, the minimum level you must restore those processes to and in what timeframe. If you know your organization can survive with 50% of your technology up and running in a week, you won't waste resources trying to have 100% of your technology up in a day. Likewise, if you know which processes need to be recovered first, you won't mistakenly apply resources to less critical processes.

3. Create solid test criteria for your plans and suppliers

The recovery requirements identified in your BIA (dependencies, required resources, maximum allowable downtime, and so forth) become the test criteria by which your recovery plans, and those of your critical suppliers, must be judged. Without this benchmark you'll have no truly accurate way to gauge if your recovery strategies will be effective. Once again, you'll only be guessing—not something you want to rely on when a real disruption occurs.



Example continuum of escalating recovery strategies

Prerequisites for a successful BIA

Get senior management buy-in

You must get top-down support of your BIA effort to be successful. To do a BIA properly takes time and concerted effort. It takes staff away from their daily activities. Without the support of top management, you'll have a very tough time convincing staff it's worth their time to participate.

1. **Make your case.** Approach top management with a good executive summary. Recap the reasons the organization has bought into BC planning in the first place. Review the threats uncovered in the risk analysis and reemphasize the potential consequences of those risks. Explain how the BIA will be used with the risk assessment to provide the basis for an effective recovery plan.
2. **Explain the process.** Let management know how you'll work with departmental staff to gather the requisite data while minimizing the impact to their work day. Show how you'll help employees share in and take ownership of the BIA process.
3. **Show how the BIA can be used in other ways.** Your BIA will provide useful information not just for your business continuity plan, but for other important business activities, including vulnerability assessments, application assessments, risk management and incident response. The BIA can help identify outdated technologies, unrealistic spending, integration issues with other organizational groups, opportunities for business process improvement, redundancy of effort and outsourcing issues. In other words, there are many ways to optimize the return on investment in your BIA effort.

Make it part of the culture

Your BIA isn't a one-time project to complete and put on the shelf. To be successful, your BIA must become a way of life at your organization, a part of your corporate culture. Circumstances and technology constantly change, and so must your BIA. This requires regular revisiting of the BIA to keep it fresh and accurate. This can only happen if it is part of your corporate way of life. The surest way to make this happen is to involve everyone in your organization in the BIA process, from every department and discipline, from top management to entry-level staff. We'll talk more about this in the data gathering section of this paper.

Keep it simple

Many companies have the mistaken notion that a BIA should be as comprehensive as possible, covering every possible contingency and process with multi-decimal point accuracy, and that getting there requires a lengthy and tedious process. Most staff don't have the patience to endure this and won't participate. Even if you manage to complete this process, by the time you're done, you may already have to revalidate the BIA after such a large amount time.

On top of this, a 1000-page manual is the last thing you want to wade through when a crisis occurs and every second lost means serious damage to your organization. A simple, short BIA based on good data will get the job done. Indeed, even a one-page BIA can be effective if it includes accurate information about your organization's business processes, dependencies, impacts of disruptions, resource requirements and recovery timeframes.

Consider having a professional lead the BIA process

To get the most objective analysis possible, you'll want to have a professional guide your staff through the process. Employees typically see processes and prioritize them within the context of their own departments. A professional can help place these processes within the larger organizational context. While your professional can be an employee of your organization, hiring an outside professional offers additional advantages. First, an outside professional can provide a more objective view. Secondly, it will be easier to get buy-in for the BIA process because top management has committed resources to having the third-party professional there.

Data gathering

What data?

The BIA requires the following information:

- All business processes performed by each department
- Resources required by each process to function properly—technology, supplies and people
- The interdependencies of processes within departments, across departments and with third-party vendors
- The financial and operational impacts to the organization of disruptions to processes (plus additional types of impacts which we'll cover shortly)—i.e., how critical is each process to the health and survival of the organization?
- The maximum allowable downtime (MAD) for each process to ensure the survival of the company, also known as the recovery time objective (RTO)
- The recovery point objective (RPO) for each process—how current does the data used by that process need to be? Yesterday's backup? Up to the minute?

Data gathering methods

1. **Questionnaires** – The most common method for gathering data is the questionnaire. Questionnaires are useful for soliciting information from many people, especially when it may be difficult to gather everyone for real-time interviews. Questionnaires are also easy to administer to a lot of people simultaneously. Like all surveys, BIA questionnaires must be carefully designed to ask the right questions and be easily understood, not open to wide variances in interpretation. While questionnaires are useful, they shouldn't be your sole data-gathering tool. Going back to our medical analogy, filling out a BIA questionnaire is like filling out a patient history. It provides useful background to the physician but doesn't take the place of a physical, x-rays, blood tests and one-on-one interviewing to diagnose your symptoms and select the proper treatment. Similarly, you should arrange time to meet face-to-face with your organization's staff to clarify answers and turn subjective answers into more objective analysis. Questionnaires also take time to fill out, and people may not be motivated to take time from their busy day to complete them.
2. **One-on-one interviews** – These allow you or your professional to more actively engage your staff, to probe, and to structure questioning on the fly to get the required information. However, depending on the size of your organization, this method may be overly time-consuming.
3. **Group sessions** – Group sessions are an excellent way to actively engage your team and reach consensus on the information you're gathering. Through lively discussion and pooling of knowledge and experience, your team will produce better data for your organization's BIA. By actively participating in the process, they'll take more ownership of and pride in their BIA. Here are some tips to get the most from your group sessions:

   a) **Involve as many people as possible.** Get everyone from each department to participate, including every function. Encourage all to contribute their opinions. This will give each person a sense of ownership and commitment and allow you to tease out more complete information.

   b) **Include both business people and IT people.** These two groups rarely communicate enough. By working together, IT staff will get a clearer picture of the expectations of their business counterparts, while business folks will better understand the capabilities and limitations of their current IT infrastructure and adjust their expectations accordingly.

   c) **Keep it short and make it fun.** Most group BIA sessions can be accomplished within an hour-and-a-half. This minimizes the impact to your staff's work day. A good facilitator will keep it interesting and fun and will keep the group's focus on what's most important without getting mired in minutiae.

d) **Be consistent.** Conduct your sessions with different departments in the exact same way every single time. This will make the experience common across the organization and give everyone the same frame of reference for future discussion.

e) **Identify processes, not procedures.** The BIA is concerned with what your team does (processes), not how they do them (procedures). Keep the discussion focused on processes. When the BIA is completed and you're developing recovery strategies, you'll then identify alternative procedures for accomplishing processes, such as using failover data centers or switching to manual procedures until your technology is back up.

Impact assessment

For each of your identified processes, you'll want to assess the impact to your organization when that process is disrupted, and how that impact intensifies the longer the disruption persists.

Assess impact, not causation

It's called a Business Impact Analysis, not Interruption Causation Analysis. In other words, it doesn't matter if it's an earthquake, flood, tornado or simply a careless construction worker down the street that interrupts power to your business. All that matters is the impact: the power is out indefinitely and your critical processes are not functioning. With this in mind, you can focus on what would happen to your business if any of your processes stopped functioning for any amount of time.

Impact scenarios

The common impact scenarios you'll likely encounter at some point are:

1. **Loss or denial of physical access.** Your technology is working, but you can't gain access to your facilities. Perhaps there was a fire, or a water main burst and your street has been closed down. Now you must decide what to divert, whom to divert, and to where, in order to continue carrying out vital business functions.
2. **You have physical access, but technology isn't working.** What are your workarounds? Can you source technology from an alternate site? What manual procedures do you have in place? Example: you're a bank. Your computers are down. A customer walks in to make a large deposit. Your manual workaround procedure might be to pull out a calculator and write out a manual receipt.
3. **Both of the above.** Commonly known as the "smoking hole" scenario, you may have a situation where your building has been destroyed or rendered uninhabitable, and the technology inside rendered useless. Your customers may be more forgiving in this type of a situation, but regardless, you have to find ways to get critical processes up and running to a minimum capacity within a certain timeframe to keep your business viable.

Impact categories

The typical BIA talks about financial impacts and operational impacts. Depending on your type of organization, there are other types of impacts you should plan for as well. A good working list includes:

1. **Financial** – Direct capital outlay to recover and loss of revenue. Example: British Petroleum's financial exposure for the 2010 gulf oil spill is in the multi-billions of dollars.
2. **Operational** – Your ability to carry out functions based on available resources and dependencies on other processes. For instance, the escrow department of a mortgage company depends on the appraisal department in order to close escrow. Or, an assembly line can't produce a widget without a small part provided by another department. Interdependencies are critical to assessing operational impact.
3. **Legal and regulatory compliance** – Can your organization be prosecuted, fined or sued as a result of processes failing to function, and if so, what is the potential liability?

4. **Impact on your customers** – How will they be affected? Can you meet your service level agreements to them? Will they defect to your competitors?
5. **Reputation** – What will happen to your organization's good will, brand equity and stock value? Example: In the aftermath of the 2010 gulf oil spill, British Petroleum's stock value sunk to half its value and its name may be forever linked with the tragedy.

Impact severity

Regardless of the type of impact, look at its severity—is it low, medium or high? This will be the basis for forming your recovery requirements. Obviously, those with higher impact severity will demand quicker attention.

Interdependencies

It's important to understand how an interruption to one process may affect other processes when estimating the maximum allowable downtime. For instance, you may decide that the maximum allowable downtime (MAD) for critical activity A is one day, while the MAD for activity B is two days. However, you may find that activity A depends on activity B for its recovery, so in fact the MAD for activity B is one day, too.

Interdependencies also include such resources as telecommunications, IT, transportation and delivery services, shared physical facilities, equipment, hardware and software, third-party vendors and back-office operations. All of these must be identified and quantified in terms of their importance to each business process.

Recovery requirements

Generally, your recovery requirements can be quantified with two measures: RTOs and RPOs. You'll also need to know what resources will be required to restore your business processes.

RTO: recovery time objective

The RTO, also called the maximum allowable downtime or MAD, tells you the length of time you can go without a critical process before your organization starts to suffer irreparable harm. The more time that passes, the greater the impact to the organization. What is the acceptable time window? Days? Hours? Minutes? By understanding the RTO for each process, you'll be able to prioritize resources to restore those processes with lower RTOs first.

Think about your RTOs as the length of time from the point a disruption is discovered and declared, as opposed to when it actually occurred. Why? Because practically speaking, until the disruption is discovered, there's nothing that can be done about it. Your RTO can only measure the time window from the moment a disruption is known to the point at which you recover your process.

RTOs differ by organization, departments and functions, but a typical scale is:

- Current business day
- Tomorrow
- In three days
- In one week
- Beyond a week

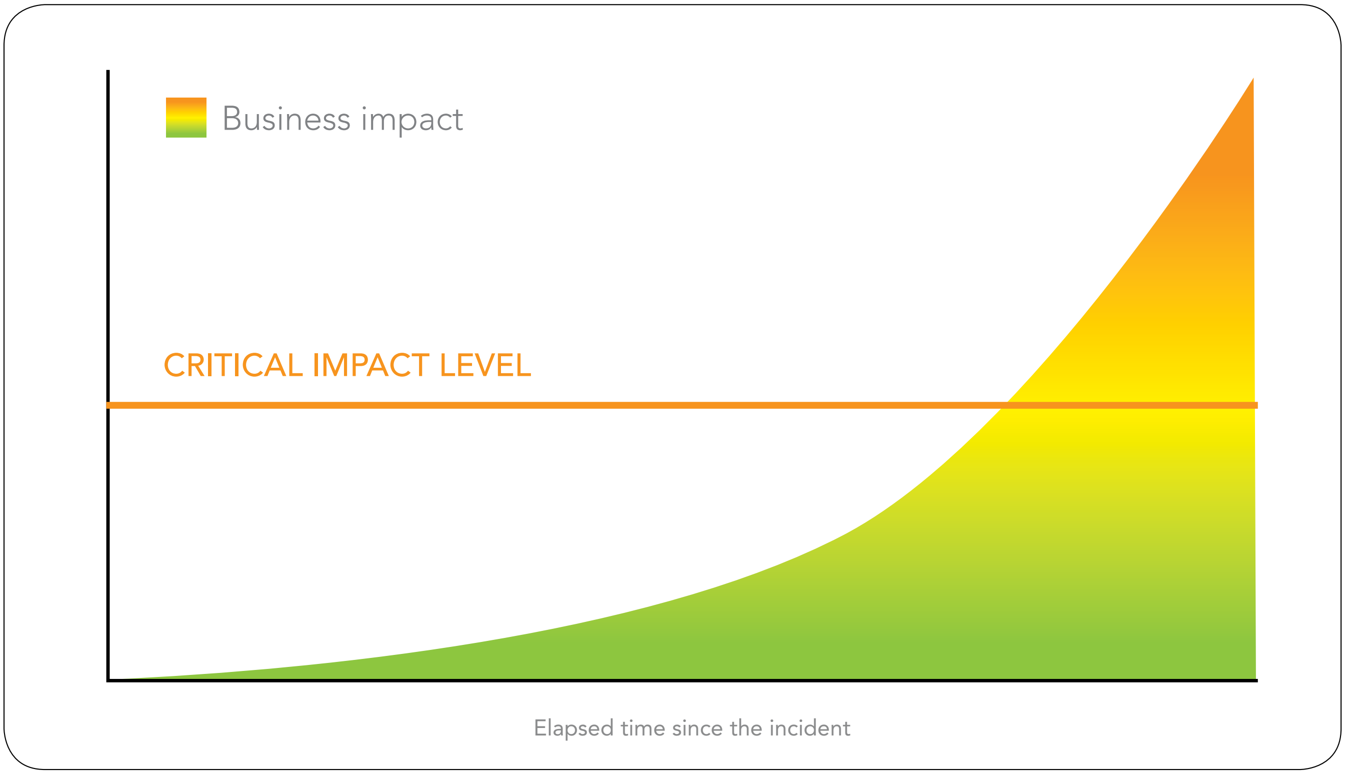
For those processes with an RTO of "current business day," further break those RTOs down to one hour, close of business, and any point in-between.

You can also think about full recovery versus partial recovery for each process. If a partial recovery in the short term is enough to keep your organization

1
2
3
4
5

running, you can then allocate remaining scarce resources to recovering other processes. And RTOs may vary by the season. If business volumes are cyclical, with peak periods and lulls, the urgency to recover certain processes may fluctuate accordingly.

Quantifying and ranking your RTOs for all processes will allow you to see at a glance which processes require attention first and to allocate your recovery resources where they're most needed.



RPO: recovery point objective

For those processes that rely on data, how current does that data need to be once it's restored? If your organization is a financial institution, perhaps your data must be current within the past hour. On the other hand, if you're a manufacturer or retailer, maybe last night's backup is sufficient. Understanding your RPOs will help you determine the minimum investment you need to make in systems to recover technology.

Recovery resources

What types of resources (technology, supplies, people, vendors) need to be in place to restore each process? Knowing these in advance will help you locate and activate those resources quickly when a disruption occurs as part of your recovery strategy (as covered in the next chapter, *Think it Through: Strategy, development and documentation*.)

Completing a BIA matrix

You'll want to use some sort of spreadsheet to compile all the information you've gathered through your BIA process and tailor it to the needs of your organization. A sample BIA spreadsheet could include the following columns:

1. Business function name
2. Business function definition
3. Business unit
4. Outage durations:
   - One: from 0 to 12 hours
   - Two: from 12 to 24 hours
   - Three: from 24 to 72 hours
   - Four: from 72 hours to 1 week
   - Five: over 1 week

   a) Financial impact (low, medium or high for each level of outage duration)

   b) Operational impact (low, medium or high for each level of outage duration)

   c) Regulatory or legal impact (low, medium or high for each level of outage duration)

   d) Customer impact (low, medium or high for each level of outage duration)

   e) Reputation impact (low, medium or high for each level of outage duration)
5. RTO
6. RPO
7. Dependencies
8. Can IT meet RTO?
9. Technology RTO

Finalize your BIA

Once you've created your BIA by department and for the entire organization, have it reviewed by upper and executive management to put all assumptions through a final test. When all parties have reviewed and approved the BIA, publish it in document form and distribute it to the entire organization. After all, if you've followed these steps, everyone will have had a hand in creating your BIA. As collective owners of it, they'll be very interested in receiving it, and they'll all have it at the ready when a disruption occurs.

Summary

Having a BIA is essential to business continuity. Having a well-constructed BIA is essential to creating effective recovery strategies. Your BIA helps you understand all of your business processes, which ones are critical, and how long your organization can survive without them. It also helps you understand how processes and resources depend on each other. And it will help you make the best allocation of limited resources to keep your critical processes running in the event of a disruption. Your BIA eliminates the need to guess, helping you make good decisions when a crisis occurs. And finally, it creates the basis for evaluating and testing your recovery strategies.

CHAPTER 3

Think it Through: Effective strategy, development and documentation

Think it Through: Effective strategy, development and documentation

CHAPTER 3

Situation

By now you've completed your risk assessment and business impact analysis (BIA). Taken together, the risk assessment and BIA identify the risks and impacts of interruptions to your critical business processes. This information provides the basis for completing the next step in the methodology: developing appropriate recovery strategies for critical business processes and writing a plan to ensure continuity.

Need

To prepare for a business interruption, you need a comprehensive plan that considers risks, impacts, and step-by-step recovery strategies in various disaster and emergency scenarios. Without a plan, your team will be flying blind when an interruption occurs. The plan provides tools to manage interruptions and resume operations quickly, aiding decision-making and making it easier to take action when there is scant time and stress levels are elevated.

Challenge

Using the information in the risk assessment and BIA you must create effective recovery strategies for critical processes in all departments. You'll incorporate these into a comprehensive business continuity plan and encourage ownership of the plan across the organization, ultimately achieving the highest resiliency possible with the resources you have at hand.

Solution

To create effective recovery strategies you'll want to look at your organization department-by-department, process-by-process. Use a template to document your recovery strategies to ensure process consistency across the organization. Finally, have plans reviewed and approved by department heads and distributed to all employees to encourage their engagement.

Results

Each department in your organization will have an action plan for business continuity outlining the steps to recover vital processes in any emergency scenario. All employees will have their own copy of the plan, ready to use immediately when a disruption occurs. This way employees will take ownership of the organization's business continuity effort and this effort will be further ingrained in the organization's corporate culture.

Recovery strategies.. 33
The recovery continuum.................................... 33

The recovery strategy development process.... 34
Department-by-department, process-by-process... 34
Use a template... 34
Sample template... 34
Write procedures to skill set............................ 35
Manual procedures... 35
Technical procedures.. 35
Alternate worksites... 35
Staffing issues.. 36

Incident response.. 36

Crisis communication....................................... 37
Dealing with the media..................................... 37
Documenting the incident in progress............. 38

Developing the plan... 38
Create plans by department............................. 39
Get departmental sign-off on your plans.......... 39
Distribute plans to everyone............................ 39

Summary.. 39

Recovery strategies

Your BIA documents your critical business processes and their dependencies. This allows you to create strategies for recovery of these processes after a business interruption because you've prioritized those processes, clearly identified everything they need to function, and determined the amount of time you have to restore them to maintain operations at a minimum required level.

Your recovery strategies will allow you to:

- Respond to a disruption as soon as it occurs
- Recover critical functions
- Recover non-critical functions
- Salvage and repair hardware, software, equipment and facilities
- Return to your primary site for operations (if it was evacuated)

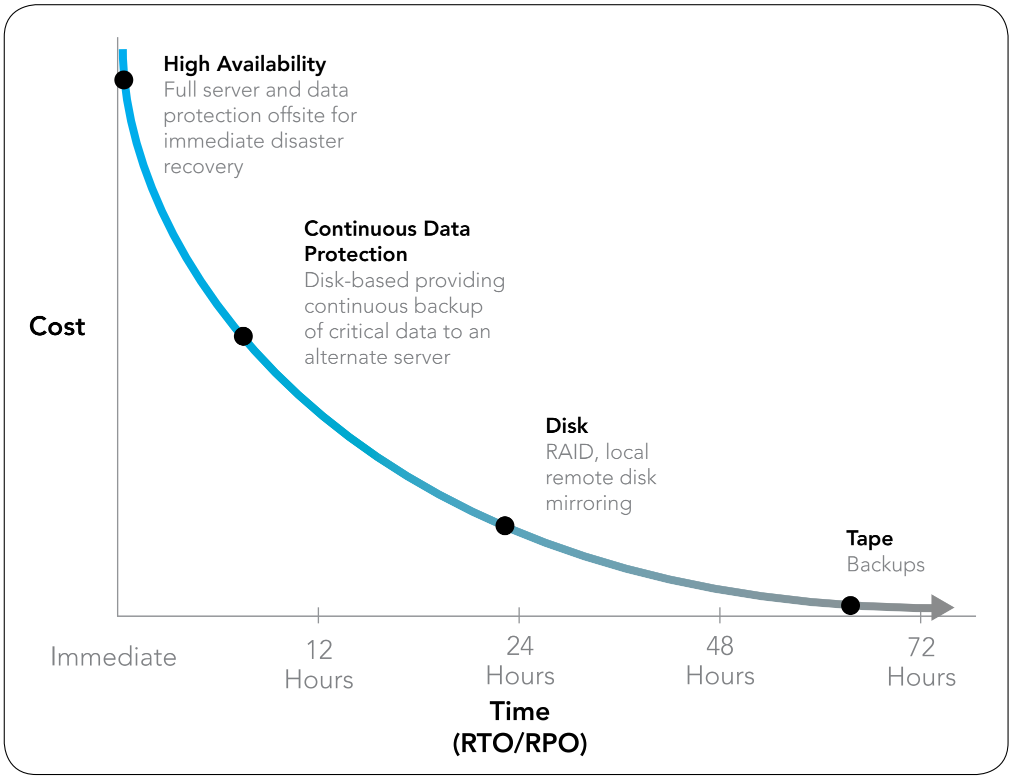
The recovery continuum

The first step in selecting recovery strategies is to perform a comparison of your organization's current IT capabilities vs. business requirements. If your current IT infrastructure cannot maintain critical processes at a minimum required performance level after a disruption, there is a gap to be filled. You next need to determine how to bridge that gap, and the cost. The level of IT capability you select depends on where you are on the recovery continuum.

Your choice of recovery strategies will depend on two factors:

1. The critical nature and maximum allowable downtime (recovery time objective or RTO) for a given process
2. The budget you have to fund your recovery of that process

These factors can be plotted on a graph, with the Y-axis representing cost and X-axis representing recovery time. An example for disaster recovery of IT functionality is in the chart below.



You can also apply this kind of gap analysis to overall business recovery strategies, with a cost/benefit analysis of options for relocation, human resources, equipment, etc.

Your team will need to determine the proper balance of cost and recovery time to meet your minimum operational requirements. This will guide the strategies you develop and implement.

The recovery strategy development process

Department-by-department, process-by-process

Just as you completed your BIA, department-by-department, process-by-process, you'll do the same with your recovery strategies. Each department should develop recovery strategies for its critical processes, based on the recovery time objectives (RTOs) and data recovery point objectives (RPOs) identified in the BIA. As you go through the process of documenting your strategies, you'll actually be writing a key section of your business continuity plan at the same time.

As you go through the process of documenting your strategies, you'll actually be writing a key section of your business continuity plan at the same time.

Use a template

The process for documenting recovery strategies should be absolutely identical across departments to ensure that anyone reading the resulting documentation will already be familiar with how its information is organized. The goal is to minimize the need to relearn anything in the critical moments after an emergency develops. Using a template to document your strategies will ensure consistency, thoroughness and familiarity of your documentation. You'll want to duplicate this template for each critical process within each department.

During an emergency, your recovery strategy template does double duty as a progress-monitoring tool for your recovery supervisors. Having a consistent format for describing procedures across all departments simplifies seeing at a glance how the recovery effort is going compared to the plan.

Sample template

Your process recovery template should include the following pieces of information:

- **Functional description:** a high-level overview of the functions of the process
- **Dependencies:** which people, resources, systems and applications, both internal and external, are required for each critical process to function at the minimum required level?
- **Recovery team contacts:** primary, alternate team leaders, team members and key vendor contacts, such as your data center
- **Recovery objectives:** RTO, RPO, estimated recovery time and restore method to be used. Also describe the state of the process after recovery; can we expect a gap between the recovered state and the normal operational state? You may have to live with a "new normal" for a period of time
- **Recovery procedures:** step-by-step recovery procedures, with columns for documenting recovery during a real incident. List procedures for pre-recovery, starting your recovery, testing the recovered process, falling back to the original process, and post recovery

By going through this exercise, you will have documented a key piece of your business continuity plan for your departments: their recovery procedures and the personnel responsible for carrying out those procedures.

Write procedures to skill set

When writing your recovery procedures, keep in mind the skills, knowledge and experience of the people who will be tasked with carrying out these procedures. Write in plain language, including only the level of technical information and jargon required to simply explain what to do. Task descriptions intended for entry-level employees should not be peppered with higher-level descriptions, terminology and acronyms. Conversely, if a highly technical procedure is being written for someone like a database administrator, then the description should contain the technical information required for the DBA to quickly understand exactly what to do.

Manual procedures

As you create recovery procedures, start with manual procedures for carrying out key functions while recovery is underway. This is critical if the time to recover a process will be longer than your RTO for that process. In that case, a manual workaround is mandatory to stay in operation. Manual procedures are also the least expensive workarounds to implement. And they are good training tools, helping staff understand how each process works, no matter whether they are aided by technology or not. A simple example: power goes out in a bank. The tellers must now balance their cash drawers manually. This will require either a calculator, or a pencil and paper, as well as mathematics skills.

Technical procedures

Based on where you are on your recovery continuum, identify which procedures you'll use to restore technological capability. For example, with regards to disaster recovery of your IT, you could choose from the following options, based on your RTOs and RPOs:

- Tape-based backup and restore – least expensive
- Disk-based backup and restore – more expensive
- Continuous data protection (disk-based enabling restore from any prior point in time) – more expensive still
- High-availability solutions (delivering continuous uptime with zero data loss) – most expensive

Alternate worksites

If a primary site is destroyed or rendered uninhabitable for a period of time, you'll need a predetermined solution to continue working at alternate locations. Options include:

- Employees working from home – they'll need the proper equipment and network connections
- Hotel rooms – Ideally you'll already have arrangements with hotels so you can quickly secure rooms after a disruption
- Lease an alternate site – be ready to locate and lease alternate sites for facilities, including office space, warehouse space, data centers, etc.
- Permanent alternate site – this is a site you already own or lease and operate in a separate geographic location for just such an emergency

Wherever you relocate to, you'll have to provide for IT and telecommunications, equipment and furniture, heating, ventilation and air conditioning (HVAC), supplies and transportation. You'll also want to choose a location far enough away from the primary site to be unaffected by the circumstances that closed your primary site.

Staffing issues

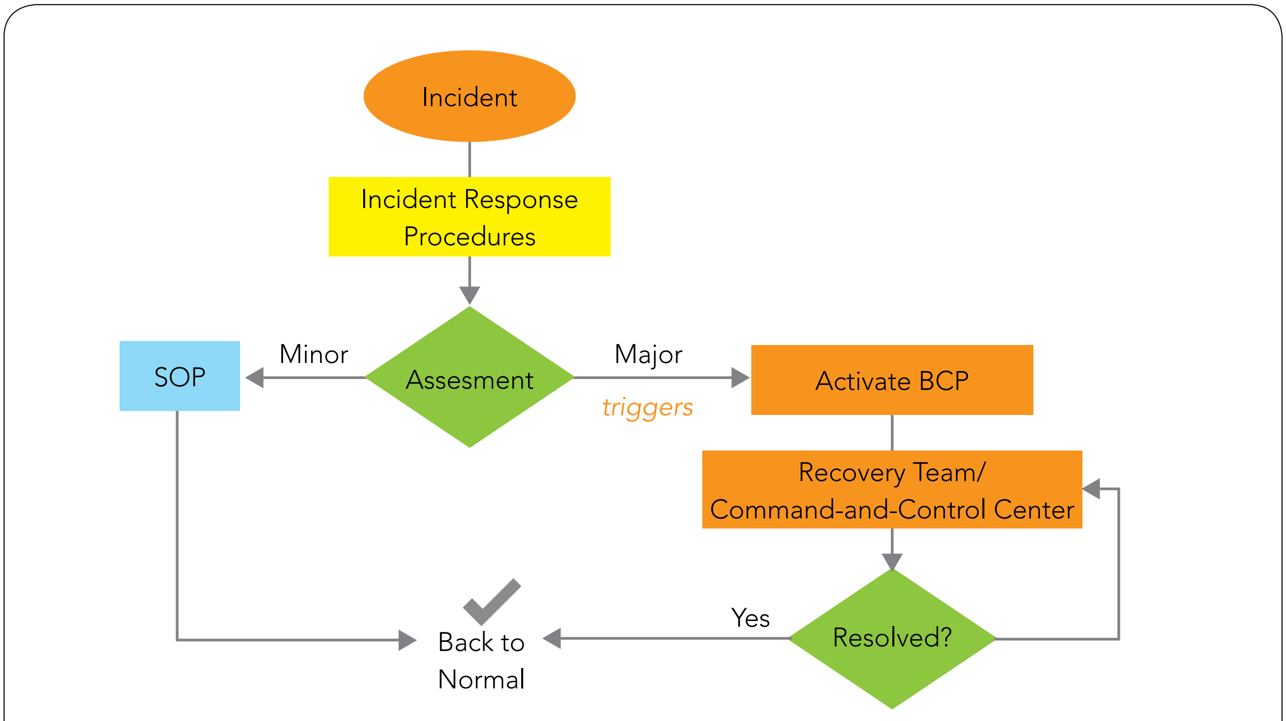
Your staff are, of course, more important than anything else. Should a disaster or severe disruption occur, you'll have multiple staff issues to deal with in short order. Some examples:

- Medical issues: was anyone injured? What first-aid capabilities are in place? How quickly can emergency medical response arrive?
- Notification of family members in case of injury or death of employees
- Evacuation: you'll need a well-documented and rehearsed procedure for evacuating and accounting for your personnel, as well as ancillary issues such as retrieving personal items like car keys left behind by staff
- Crisis counseling
- Transportation of your evacuated staff: from the affected site to alternate work sites as well as to and from their homes
- Relocation to alternate sites: including badges or security access procedures, other work assignments, etc.
- Daycare services for the children of displaced staff, particularly if they are forced to work an extended distance from their homes
- Housing such as hotel rooms if staff must be relocated
- Personal expenses and per diems for staff using personal funds for food, lodging, cell phone use, Internet hook-up, etc. while under relocation
- Payroll

Incident response

At the onset of a disruptive event, your incident response team will jump into action. This team's job is to assess the situation and respond using a step-by-step procedure based on the severity of the situation. Activities include evacuation, notification of key personnel and activation of the business continuity plan. If the plan is activated, recovery teams will be assembled and a physical command-and-control center will be set up to direct the recovery effort.

It is important to carefully consider and define triggers for activating the business continuity plan to ensure the plan is used when needed. An example will illustrate this crucial point. Consider the organization that defined a disaster as something that impacts 100 users and used that as its trigger for activating its business continuity plan. One day a switch went out, impacting over 100 users. This constituted a disaster by definition; however, averting the disaster required simply replacing the switch. In another instance, the same organization experienced a flood that resulted in massive damage but only impacted 80 users and so was not deemed a disaster and the business continuity plan was not activated!



A typical flow chart for incident response

Crisis communication

When a disruption occurs, it's critical to be able to communicate with all personnel to ensure their safety and coordinate their activities during the recovery effort. Traditional phone trees take time, tie up resources and are open to human error. Many organizations today use an automated mass notification and response system to expedite two-way communication with all personnel. Such a system automates the communication process to reduce the chance of human error, can contact thousands of people in minutes, and uses multiple modes of communication to eliminate single points of failure and reach employees wherever they are.

It is also critical to maintain contact with stakeholders, relatives of employees, and local public safety agencies, as well as regulatory agencies in the case of regulated industries such as finance. Just as important is contact with key vendors that critical processes depend on.

Dealing with the media

Your organization will likely have to answer questions from the media during a crisis. Your plan should specify which personnel are authorized to speak to the media, and guidelines for what to say and how to say it should be spelled out in the plan. Authorized personnel should receive media training for dealing with the press appropriately. This point cannot be over-stressed. Two examples illustrate the point. The first is that of an organization which initiated an evacuation after a natural disaster. When talking to the press, the spokesperson said that all but one employee had been accounted for. Upon hearing this news report, families of the organization's employees immediately wondered if it was their family member that was missing, causing unnecessary stress. In the second example, the CEO of British Petroleum was given notice in the summer of 2010 following the company's massive gulf oil disaster after he made seemingly callous statements to the press.

Documenting the incident

Designate one of your staff people, ideally the senior administrative staff person attached to the highest ranking supervisor in your command-and-control center, to be your incident scribe, documenting actions taken by authorized personnel in accordance with your business continuity plan. This not only provides valuable feedback for improving response and recovery in the future, but also provides proof of the actions your team took to safeguard the company should there be an inquiry after the fact.

Developing the plan

With your recovery procedures documented, you're well on your way to completing your business continuity plan. The recovery procedures are the heart of the plan. Now it's time to flesh out the plan. In total, your plan provides a blueprint to follow from start to finish when a disruption occurs, minimizing the need for ad hoc decision making when time is short and stress levels are high. The plan includes:

- Initial response to a disruption (a.k.a. incident response)
- How to determine when to activate the plan
- Recovery team structure and location (your command-and-control center)
- Who to contact, how to contact them and what to tell them
- Subsequent tasks to carry out (recovery procedures):
  - Who does them
  - How they do them
  - With which resources
  - Using which skill sets
  - In what time frame
- Crisis communications
  - Internal
  - Vendors
  - Stakeholders
  - Public safety
  - Regulatory agencies
  - Relatives of employees
  - The media
- What to do after recovery
- Salvaging facilities and operations
- Resumption of business as usual

A typical business continuity plan is organized in the following way:

- Executive summary
  - The purpose of having the plan
  - Assumptions:
    - + Plans usually assume the worst-case scenario to provide readiness for any type of disruption
    - + What procedures and resources are available to carry our recovery strategies
  - Definitions
    - + Terms: “command-and-control center” “alternate site,” etc.
    - + Triggers: what constitutes a disruption necessitating activation of the plan
- Risk assessment (the first step in the business continuity methodology)
- Business impact analysis (BIA; the second step in the business continuity methodology)
- Team structure (including complete contact information)
  - Incident response team
  - Business recovery team
  - IT recovery team
- Incident response plan
  - Emergency assessment and response
  - Evacuation procedures
  - Emergency medical response
  - Triggers that activate the BC plan
  - Incident response flow chart

- Recovery strategies (including, and not limited to):
  - Prevention strategies
  - Notifications (staff, stakeholders, vendors, authorities)
  - Facilities
  - Equipment and supplies
  - Data processing
  - Network
  - Telecommunications
  - Public relations
- Plan distribution
- Plan maintenance and version control
- Plan testing (to be covered in chapter five)

Create plans by department

While many companies will create an all-encompassing plan for the entire organization, the larger your organization, the more unwieldy this can become. Consider having individual plans by department, and if practical, creating more specific plans by location within departments. This way, recovery teams only have to deal with strategies that are specifically relevant to their processes, people and locations, using the most concise possible plan to streamline access to critical information when time is of the essence.

Get departmental sign-off

Once your plans are developed, it is critical to have your department managers review and approve the plans. This not only confirms that all information is accurate but further encourages managers to take ownership of their plans.

Distribute plans to everyone

Remember, business continuity planning only works if it is an integral part of the corporate culture. The way to help ensure this is to include everyone at every step, and plan completion is no exception. When your plans are complete, be sure to distribute them to everyone. This way, everyone has visibility of the results of their hard work and will more readily take pride and ownership in the plan. Equally important, all employees will have their own copy of the plan, ready to use the moment an emergency starts to unfold. There are many methods for distribution, including hard copy, PDF and company intranet. Consider also distributing a PDF copy of the plan on USB thumb-drive key chains so people have the plan wherever they go. The keychain will serve as a constant reminder of emergency readiness for all employees.

Summary

Your organization's risk assessment and BIA identify the risks and impacts of interruptions to your critical business processes. This information, combined with your available budget and resources for responding to interruptions, provides the basis for developing appropriate recovery strategies and writing a plan to ensure continuity of your business operations. This guide has provided you with a framework for this step in the business continuity planning methodology—consider this framework a skeleton. It is up to your team to flesh out a comprehensive response plan. There are many third-party software tools available to assist you with developing your strategies and plan as well as implementing them. Chapter four will provide an overview of that information.

CHAPTER 4

Your BC Toolkit: Options and integration

Your BC Toolkit: Options and integration

CHAPTER 4

Situation

By this point you have completed the first three steps in the business continuity planning process: the risk assessment, the BIA, and the evaluation of budget and resources for responding to interruptions. From these, you've developed the appropriate recovery strategies for your critical business processes and should have at least begun to document your plan. Now you need tools to augment and streamline the process. To choose the right tools you must understand the unique needs and the corporate culture of your organization.

Need

Developing a BC plan is an ongoing, growing and changing process. To manage this you'll need tools that help you document your plan and keep it up to date. Tools can range from simple solutions like a printed document or a spreadsheet to a full-fledged, all-in-one business continuity toolkit with templates, document management tools, a version control system and more. No matter what you decide, remember that the tools are not the solution itself, and there are no shortcuts.

Challenge

The biggest challenge is in assessing the real needs of your particular organization and determining the tools that will work best. That requires a full understanding of the organization and its culture. Could a one-size-fits-all solution work for your company? Can you choose a less cumbersome and less costly SaaS solution or will the particular constraints of your organization dictate a higher level of control?

Solution

Fortunately, there are many options, whether for document management, BIA, incident management, command and control, audit, notification and communication, crisis management or recovery. We don't recommend specific solutions or vendors, but we'll explore the types of tools and guide you through assembling your own BC toolkit.

Results

When your toolkit is in place and you follow the process as outlined in this program, you will be prepared to roll out your plan, test its vulnerabilities and be fully-prepared for interruptions, no matter what form they take.

What to expect from a tool............................ 42
Understanding corporate culture...................... 43
What are your company's show-stoppers?........ 43
Tools and how to choose.................................. 44
Preparatory or planning tools........................... 44
Event management tools.................................. 45
Delivery options for tools.................................. 45
Review of tools/features/benefits...................... 46
If you choose to use a consultant...................... 46

Summary.. 46

1
2
3
4
5

What to expect from a tool

The first thing to understand when choosing your business continuity tools is this: a tool is not a solution nor is it a panacea. Just as a typewriter or word processing program may seem essential to producing an effective and powerful report, the typewriter or word processor is merely a tool—it does not write the report. After a great deal of research, information gathering and thought, you use the tools you've chosen to produce the report. It's the same with business continuity planning success—after doing your homework, you can use your carefully selected tools to implement your well-thought-out plan.

Going back to the typewriter analogy: what happens when you make a mistake? You have to either use Wite-Out to cover up the mistake or you have to tear up the page and start over. Again, it's not the tool that made the mistake. This chapter will help you ask the right questions and figure out what tools you'll need in your BC toolkit so that you won't have to cover up mistakes or start all over again.

A typical mistake made when choosing business continuity tools is the assumption that the tools will determine or even drive the plan, when in fact, it's the other way around. It's sometimes assumed that the tools will reduce headcount, obviating the need for someone who regularly maintains the plan and implements it when business is interrupted. This is simply not so. Good tools don't replace people, but they do empower them. You still need to have solid planning and good management behind the solutions you choose.

Choosing the right solution for each element of your BC plan is critical. If the tool is not right, the organization has to change to match the tool rather than the tool matching the organization, much like the square peg trying to fit into the round hole. Often people make the wrong decision because they're impressed by a vendor's splashy presentation or big name, and they end up discounting the importance to the culture that the tool should serve. Once the wrong tool is chosen, no one wants to admit they made a mistake, so they tend to invest even more in the product, trying to make it fit. It's hard to go back and cut your losses, as the tendency is to keep moving forward no matter what, digging in deeper rather than admitting defeat and making a better choice. Often the weakness or mismatch of a particular tool only gets revealed in the heat of a crisis, so it's wise to carefully consider all the options and choose carefully.

> Often the weakness or mismatch of a particular tool only gets revealed in the heat of a crisis, so it's wise to carefully consider all the options and choose carefully.

This is not a time when you can cut corners, but must focus on your goal of finding the right tool for your company. That means getting the most you can get out of your budget and finding a tool or set of tools that really fit your organization. Customization is costly and time-consuming and should only be relied on when the right solution can't be found. And even the best tools, if too clumsy or cumbersome to use, will end up being left on the shelf when needed.

A common statement heard in the BC world is: "The time we liked our tool best was the day we all sat down and watched the demo." That suggests the team was introduced to a great tool (and it probably really was a great tool—for someone) and watched it work under the best possible circumstances so it looked great. It helped them see what it would be like if all plans and strategies were in place, and their needs were an exact match for the fictional company that was portrayed during the product demonstration. It would be great if your company were just like that fictional company, but we all know that is rarely the case. Every company is unique, with its own requirements, limitations, desires and expectations.

Understanding corporate culture

Corporate culture is a term used to describe the psychology, collective beliefs, attitudes, values and processes that give your organization its unique personality. Some organizations are conservative, others are edgy; some are reliable and others are innovative, some are a combination of all of the above. But each company is unique and that uniqueness is what is referred to as corporate culture. In order to put a solid BC toolbox together, it's essential that you really understand what is important to your company, culture-wise, before you choose your tools.

Many organizations unwittingly foster an us-against-them mentality, whether that the conflict be between sales and marketing, executives and managers, or product team A versus product team B. That can be a challenging situation to address. On top of that, often the person who is in charge of developing the BC plan is chosen against their will, a "stuckee" who is working outside of his or her core competency, and without executive support, and may not even be the best person to choose the business continuity planning solution. Even an outside consultant who doesn't fully understand the organization can get caught up in this divisive ethos and needs to make an effort to be brought in as a partner in the process rather than as an outsider.

Corporate culture is a term used to describe the psychology, collective beliefs, attitudes, values and processes that give your organization its unique personality.

One technique you can use to keep things objective is to get as many people as possible involved in the process. Each additional person will broaden the group's understanding of the corporate culture, providing further insight and increasing the chances for success. The plan will change from being the "stuckee's" plan to the team's plan. Everyone will root for the success of the plan and will contribute to making the right choices. Garnering involvement and support from all quarters also helps win over the people within the organization who tend to be the most disagreeable, those that it's hardest to win approval from, the spoilsports. If you involve enough supporters, the BC plan and all the tools associated with it will become ensconced in the culture of the company. Get as many people in the company involved as possible.

What are your company's show-stoppers?

Another way to get to the heart of the culture is to consider what your company might call show-stoppers. Consider this carefully—what are the things that right up front aren't going to work for your organization?

It may help to compare this to the dating game. There are things you'd like to have in a mate, things you're flexible about, things that really annoy you, and then there are show-stoppers. For instance, say you're dating a person who is perfect in every way, except for one thing. You know, deep inside, that your reasons for deciding that this thing is a show-stopper are valid for you, but since this person is so very likeable in so many ways, you decide to move forward with the relationship. You become more and more invested in the relationship, but at the same time, this one thing is holding you back from being truly committed. Eventually the talk about marriage comes up and that's when you have to come face to face with the situation—are you prepared to spend the rest of your life with a show-stopper? It is easier to end the relationship before you have a lot of time, energy, and emotion invested. It's the same for BC planning—don't let things go too far in the wrong direction when choosing the tools for your plan. Know your show-stoppers.

Following are some typical corporate show-stoppers. These are red flags—ignore them at your peril:

1. **Inadequate security** – some companies, such as government agencies, must work with solutions that reside on their own network for security and control reasons, working through an intranet rather that the Internet.
2. **Financial imbalance** – If you work for a very large company you may want to take a look at their financials and choose not to go with a company, no matter how fine their tools, if you think they are small enough to be an acquisition target or that they may not have staying power.
3. **Database incompatibility** – If you use a different database to store your information you'll want to consider carefully if you are willing to transfer all that information to a new system. How will you keep it up to date? What if something happens and you need to take your data back, can you manage that?
4. **Organizational support** – If you suspect that your organization may need more support than is usual you'll want a larger supplier to ensure you get all the support you need.
5. **Backup systems** – How essential is a backup plan to your organization? If the vendor's backup plan isn't as strong as that required by your company, keep looking.
6. **System interoperability** – Does the vendor's system talk to your system? Can you sync the two up with minimal effort? These are important questions to ask.
7. **Reputation** – This should be a show-stopper for everyone. Ask for references in your industry, talk to colleagues at industry shows and events. If someone has a solution that they think is pretty good, but it turns out they're afraid to actually try it out because it seems complicated, take that as a negative reference.
8. **Contract terms** – Sometimes contract terms can be too restrictive for your organization, especially in the case of a hosted solution. Once the solution is deployed, how often is the contract renewed? Many contracts are month-to-month, some are year-to-year, or in some cases, contracts can tie you into a multi-year relationship with no chance to reevaluate along the way.
9. **Database ownership** – Will you own and maintain your own data or will your vendor? If you want to regain the data, how quickly can that be transferred? Will it cost you additional money? In what form will it be delivered?
10. **Certification level** – SAS 70 is one example of a certification level that is often required by large financial institutions. If those institutions use vendors that are all certified to SAS 70, they stand a much lower chance of being audited, saving tremendous amounts of time and resources.
11. **Your gut** – How do you and your team feel about the tool and the company behind it? Besides the perks they may offer, what's the sense of the company behind the products?

Tools and how to choose

As mentioned, there are many BC planning tools to choose from, ranging from tools that help you devise your plan to tools for managing a crisis or interruption. Think of your business continuity plan as a meal with many courses; each tool is a course, and when they all work together, they form a complete and satisfying experience. Just like a nice meal, the tools can be served up or delivered in various ways, depending on what you want to do with them and, again, your corporate culture.

The types of tools can be divided into two groups: preparatory tools and event-management tools.

Preparatory or planning tools

Preparatory tools are used to strategize, develop and document the BC plan and will aid in the ongoing management of your plan. Think of BC planning as a journey rather than a destination, a living plan that must be adapted as changes happen within your company. Tools that help in documenting version control and in maintaining the plan are critical when your plan is audited or tested by real-life interruptions. These tools may include:

- BC planning templates
- BIA tools
- BC planning modules
  a. Managing ongoing documentation
  b. Pandemic planning
  c. Crisis management
  d. Emergency management
  e. Event testing tools
  f. Auditing tools

Event management tools

These are the tools that get used when an event happens, when you hear the call, "Hello Houston—we've got a problem." These are the tactical tools needed to support your BC plan. It's vital that these tools work together at all times. Tactical tools assist with:

- Incident management
- Command-center management
- Notification
- Crisis management
- Communication
- Auditing

Delivery options for tools

How these various tools are introduced into the organization is important. Do they reside behind your firewall as installed software, or on the Web as a hosted or SaaS solution? Do you need to manage them through your intranet? Here are the options:

- **Homemade or clipboard tools** – These include using Word and Excel to cobble together your plan. Many people love to start with these tools as they already have them and they are familiar, but they have limitations. How do you manage the documents that are produced? How do you manage version control and ascertain that all departments create their documents consistently? Remember—your plan needs to be accessible to everyone, not just the person who devised it. Where do all these various documents reside and are they automatically backed up? Many people use common word processing software and spreadsheets to develop their plan, but it's worthwhile to check out the options and perhaps choose something more intuitive, with a standardized format and a built-in way to manage versions, testing, etc.

> Many people use common word processing software and spreadsheets to develop their plan, but it's worthwhile to check out the options and perhaps choose something more intuitive, with a standardized format and a built-in way to manage versions, testing, etc.

- **Hosted, SaaS** – A hosted solution is one that resides on the Web; there is nothing for you to install or manage and upgrades happen automatically with no action on your part. Access is available through any Web browser. The company providing the tools also handles building and maintaining the infrastructure, saving you money. Be aware that this means your data also resides outside of your control, so you'll want to know that it is secure and also how to reclaim it if necessary.

- **Installed, in-house** – An installed solution gives you more control over the data and how it is managed and shared. This can be the most secure option but also the most expensive, as you will need to manage all the internal infrastructure, including servers, a firewall, antivirus, software licenses, etc. You'll need staff to see that the system is always available and a backup plan in case your network goes down and you lose access to the tool.

- **Hybrid or one-size-fits-all tools** – These are a combination of planning and event-management tools, bundled together and sold as an all-in-one solution. This allows you to purchase your entire toolkit from one vendor, which can be an advantage as well as disadvantage. A hybrid solution can simplify your decision and generally assures that all included tools work together well, but it also removes the option for you to negotiate on price and puts the vendor in more of a decision-making role.

Review of tools/features/benefits

- Make decisions objectively and independently
- Gain the support of the team
- Consider your corporate culture
- Determine which tools are needed
- Determine best delivery model for those tools

If you choose to use a consultant

At this point, you may be considering the wisdom of using an outside consultant to assist in developing your BC plan and advising you on the right tools for the job. There are many good reasons to take advantage of the expertise a consultant can bring to the table. A good consultant will want to be part of your team, but will also be able to add necessary objectivity and will drive your team through the due diligence process. They usually have a lot of experience with negotiating both prices and contracts. A BC planning expert will be up to date on the latest tools and can be help with the complicated task of choosing which ones will work together. Best of all, a good BC planning consultant should save you more money than the fee they charge for assisting with system selection.

Summary

In closing, selecting tools for business continuity management can make or break your BC program. Organizations that have gone through the process outlined in this guide often find that they are happier with their solution and feel more confident in the choices they have made. Typically, half of the tools purchased for BC planning end up being abandoned soon after and are never used—take your time, make the right decision and you won't have that experience.

Time and due diligence need to be spent before choosing the right solutions and solution partners. If you develop subjective (organization-specific) criteria for evaluating the various solutions and perform objective evaluations you'll end up with a solution which will be accepted easily into your organization and meet your business requirements.

CHAPTER 5

The Final Countdown: Rollout, testing, and results

1
2
3
4
5

The Final Countdown: Rollout, testing, and results

CHAPTER 5

Situation

By now you've completed many of the steps in the business continuity planning process: the risk assessment, the business impact analysis (BIA) and the evaluation of available budget and resources. You've outlined your critical business processes and determined the tools needed to document and carry out your plan. All that's left is rolling it out, testing it, and then modifying, adjusting and updating the plan to suit the evolving needs of your company.

Need

As you know by now, your BC plan is a living document that must change as your organization and the environment around it changes. Reevaluating your plan in a systematic, structured manner is the only way to ensure that it's as good as it can be at any time. Testing is the critical piece that guides you in maintaining and evolving your BC plan.

Challenge

If you are the person in charge of creating and maintaining your BC plan, short of suffering a major catastrophe, how can you be sure that your bases are all covered? How do you test your plan, and how often? What factors need to be taken into consideration as your organization grows or shrinks, adopts new technologies, changes location, or any of the other myriad changes that face businesses today? You need a way to test your plan that is not disruptive to the organization and that engages your team and maintains the plan as an integral part of your company.

Solution

The key to effective testing is to adopt an attitude of exploration and discovery. These tests are not pass/fail exams, but rather a way of exercising your plans and people to reveal potential weaknesses. This chapter will take you through a variety of tests that include a checklist, a structured walk-through, an emergency evacuation drill and a recovery simulation—all highly useful in exercising your BC plan.

Results

When you have completed your testing you will be ready to roll out your plan, face auditors with confidence, and best of all, know that your plan will realistically help your organization protect its staff, its reputation, its assets and its resources.

Disaster strikes....... 49
Are you prepared for such an event?....... 49
How to maintain and update your business continuity plan....... 50
Guidelines for keeping your plan current....... 50
Plan testing....... 51
Benefits of testing....... 51
Testing your vendors....... 51
Types of tests....... 52
Test schedule....... 53
Development of your test plan....... 55
Evaluating the test exercise....... 55
Testing forms that you will create....... 56
Testing procedures....... 56

Checklist test....... 56
Participants....... 56
Procedures....... 56

Structured walk-through test....... 57
Participants....... 57
Procedures....... 57

Recovery simulation 59
Participants....... 59
Procedures....... 59

Recovery simulation – information technology....... 60
Participants....... 60
Procedures....... 60

Communications test....... 62
Participants....... 62
Procedures....... 62

Summary....... 63

Disaster strikes

On May 22, 1960, near Valdivia in southern Chile, the largest recorded earthquake occurred. It has been assigned a magnitude of 9.5 by the United States Geological Survey. It is referred to as the "Great Chilean Earthquake" and the "1960 Valdivia Earthquake." The earthquake occurred beneath the Pacific Ocean off the coast of Chile. Ground motion from this earthquake destroyed and damaged so many buildings that the Chilean government estimated that about 2,000,000 people were left homeless. It was fortunate that the earthquake occurred in the middle of the afternoon and was preceded by a powerful foreshock that frightened people, causing them to flee from their buildings and placing them outside when the main earthquake occurred. Most of the damage and deaths were caused by a series of tsunamis that were generated by the earthquake. These waves swept over coastal areas moments after the earthquake occurred, tearing buildings from their foundations and drowning many people.

Tsunamis generated by the Chilean earthquake traveled across the Pacific Ocean at a speed of over 200 miles per hour.

Tsunamis generated by the Chilean earthquake traveled across the Pacific Ocean at a speed of over 200 miles per hour. Changes in sea level were noticed all around the Pacific Ocean basin. Fifteen hours after the earthquake a tsunami with a run-up of 35 feet swept over coastal areas of Hawaii. Luckily, Hawaii's automated tsunami alert system kicked in and the sirens sounded 10 hours before the tsunami hit the islands. The technology worked as designed. But most of the people who heard the sirens did not evacuate. They weren't sure what the siren meant. Some thought it signaled they should stand by for more information. The technology worked but the preparation and training didn't. In the end, many shoreline facilities and buildings near coastal areas were destroyed. Near Hilo, Hawaii, 61 people were reported killed by the waves.

Are you prepared for such an event?

You've developed your BC plan, but you're nervous. What if something devastating, like a major earthquake were to occur—would your plan cover all contingencies? Can you test your plan thoroughly enough to put everyone's mind to rest? How often should you test, and just how do you test something that is evolving and changing, the way a good BC plan should? All of these questions are answered in this chapter.

The business continuity planning process should include regular updates to your BC plan. The plan should be updated based on changes in business processes, audit recommendations and lessons learned from testing. Changes in business processes include technological advancements that allow faster and more efficient processing, thereby reducing acceptable business process recovery periods. In response to competitive and customer demands, many institutions are moving toward shorter recovery periods and designing technology recovery solutions into business processes. These technological advances underscore the importance of maintaining a current, enterprise-wide BC plan.

Let's explore some fundamentals about testing and what we want to achieve. We're all familiar with pass/fail tests that get us something we want, like our first driver's test. Getting your driver's license means you know the basics of operating a motor vehicle, but does it really mean that you know how to drive? It's takes time and experience to become a good driver.

Testing your BC plan isn't quite like taking your driving test, nor is it like a lot of other pass/fail tests you take over the course of a lifetime. When you test your plan, rather than passing or failing, you're really testing your command of the subject and revealing which areas are weak and need more preparation. You are exercising your plan to make sure there are no hidden weaknesses—there is no failure, just evidence of areas that need more thought and preparation.

If you're concerned that you are not yet ready to test, or that you're not sure how to evaluate your results, remember—you already have metrics set out in your business impact analysis (BIA) and your recovery time objectives (RTOs). If you've followed this guide and taken the steps as presented, then your BIA and RTOs will provide objective criterion to test against.

> You are exercising your plan to make sure there are no hidden weaknesses—there is no failure, just evidence of areas that need more thought and preparation.

How to maintain and update your plan

Standard industry practices for maintaining a current BC plan include:

1. Integrating BC planning into every business decision
2. Incorporating BC plan maintenance responsibilities in applicable employee job descriptions and personnel evaluations
3. Assigning the responsibility for periodic review of the BC plan to a planning coordinator, department, group, or committee
4. Performing regular audits and annual, or more frequent, tests of the BC plan

Guidelines for keeping your plan current

Typically, the business recovery coordinator is responsible for assuring the plan is kept current. The recovery teams are responsible for reviewing and updating their segments of the plan and related materials. The recovery management team is responsible for the overall plan coverage and incident management procedures. Through the periodic review of the plan assumptions and risk assessment, the recovery management team's job is to assure the plan adequately addresses the risks faced by the organization as changes in the organization and operations occur.

Twice a year business recovery plan updates should be identified and applied. The business recovery coordinator will set the timing of these mandatory plan reviews to be least disruptive to normal operations. The recovery teams should initiate updates to the plan if there are changes in operations or recovery requirements. Using the steps included in this paper, you can create a plan maintenance form and use it as a tool to document the plan change history. The business recovery coordinator is responsible for maintaining the master change history. Individual teams can also use this form for documenting the changes identified during review of the plan document.

When revisions to the plan are made, the revision history at the end of each section being modified should be updated to record:

- Revision number
- Name of the person authorizing the revision
- Description of the change and sections affected
- Date of the change

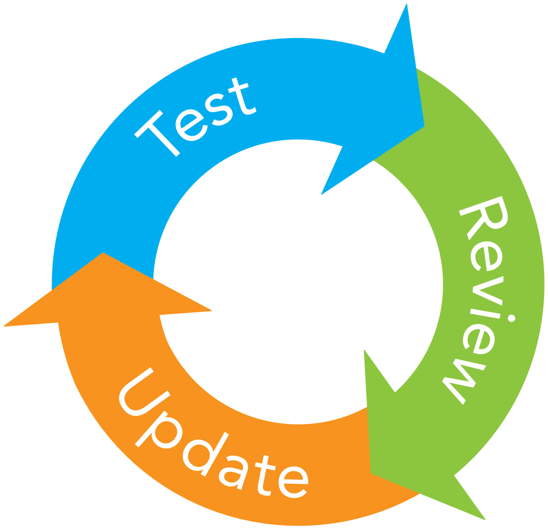
Revisions should be given to the business recovery coordinator for inclusion in the master copy of the plan and distribution to appropriate personnel.

Plan testing

An active program of testing, which is, in fact, exercising the business recovery plan, should be followed. The plan testing is designed to coordinate review and updates of the plan with the recovery management teams and other recovery teams.

Exercising the plan by the recovery teams encourages the team customers to identify potential omissions or limitations and prepares them to carry out the plan in the event of a disaster. Updating the plan should occur before and after each exercise. That way the exercise will benefit from plan enhancements, and the plan will reflect changes applied as a result insights obtained during the exercise. The diagram below illustrates the continuing cycle of plan review, maintenance and testing.

Everyone in the organization needs to understand an untested plan provides little assurance of the plan's validity or achievability. Testing is important and has powerful benefits.



Benefits of testing

- Determines the feasibility and compatibility of back-up facilities and procedures
- Verifies the completeness and accuracy of the plan
- Identifies areas within the plan that should be enhanced or updated to improve the effectiveness
- Provides a mechanism to integrate plan maintenance and improvement
- Provides training to the team managers and team customers as well as opportunities for the team leaders to evaluate the team's performance
- Demonstrates the ability of the organization to recover and build the confidence of the teams

Management, with the guidance of the business recovery coordinator, should identify the testing objectives and strategies to be employed. These objectives will change over time as the recovery teams become more proficient, the plan becomes more robust and changes in the organization or recovery strategy occur. The business recovery coordinator, working with the recovery team leaders, will develop detailed test objectives and plans for each exercise. In developing the testing program, all aspects of the plan and recovery team procedures should be fully exercised.

The five-year testing program is noted further on in this document; it can be used as a guide in the progression of testing activities. The testing program should be reviewed annually and revised to reflect the exercise results and changes in operations or risks as identified by management.

Testing your vendors

An important part of the success of your plan relies on your vendors so they are also a important element in testing your plan. How quickly can a vendor drop-ship servers and the other equipment you'll need? How good is your data storage and back-up facility, and how much time will it take to transfer the data you need to get your organization back on track? All of your vendors need to be tested, but to streamline the process they should be tested at a different time than internal resources.

Types of tests

The following types of tests may be used to conduct recovery plan exercises. The type of test you choose will depend on the experiences of your organization and the recovery teams in accomplishing the recovery using the plan and the objectives to be achieved from the test exercise. These tests include the checklist test, the structured walk-through test, the emergency evacuation drill and the recovery simulation. Let's review each test:

1. **Checklist test**
   A checklist test can assist in determining whether the plan is current, adequate supplies are stored at the backup site, telephone numbers are available, quantities of emergency forms are adequate, and copies of the plan and necessary supplemental documentation are present. Using this testing technique, the various teams review the plan and ensure key materials and supplies are available and current. Recovery teams should conduct an annual checklist test to verify off-site storage data inventories and materials.

2. **Structured walk-through test**
   This testing is typically performed on a team or departmental basis and involves a detailed walk-through of the various components of the plan by each team customer. During a structured walk-through test, the participants describe or act out their responses as provided in the plan for a simulated disaster. Normal operations are not interrupted. A disaster scenario identifies the type of disaster and the components of the plan to be tested. The disaster scenario exercise introduction should include the following information for the participants:
   - Purpose of the test
   - Type of test to be performed
   - Test participants
   - Purpose of post-test review
   - Assumptions to apply during the exercise
   - Constraints on response
   - Timing: time of the day, month and year that the disaster occurred
   - Duration of the incident
   - Extent of damage or interruption
   - Notifications that have occurred
   - Response activities to be initiated

   Testing should include notification procedures, temporary operating procedures, backup and recovery operations and other items critical to the response. During the structured walk-through test, the following elements can be examined: hardware, software, personnel, data and voice communications, procedures, forms and supplies, documentation, transportation, utilities and hot-site processing.

3. **Emergency evacuation drill**
   The initial response to an incident requiring evacuation needs to be considered as part of a disaster response and business recovery plan. The facility evacuation should be exercised annually with all personnel to assure they understand how the evacuation is to occur, procedures for handling personnel with physical limitations, external assembly locations, and how verification of all personnel is

to be accomplished. The business recovery coordinator works with the facility security personnel to arrange and carry out the evaluation drill. The inclusion of local first responder personnel (e.g., fire and police) should be planned to assure coordination of efforts and understanding of the limitations and evacuation requirements.

4. **Recovery simulation**
Recovery simulation testing is more complex, requires more planning, and involves a greater level of risk and cost to be successfully carried out. Therefore, a combination of checklist testing and structured walk-through testing should be used to determine initial enhancements to the plan before attempting more extensive exercises.

Teams participating in the simulation use equipment, facilities and supplies as they would in a disaster situation, and as provided in the plan, to carry out critical functions using the recovery and restoration procedures. The participants are presented with a scenario of the disaster and with situations that are designed to cause them to respond as they would in a disaster. The situations they are confronted with are potential situations that can be expected (i.e., request for normal service or information) and unexpected situations (i.e., team personnel are not available or anonymous calls for information). The successful conduct of simulations usually requires the help of a facilitator to provide the disaster scenario and set up the situations played by actors.

Detailed discussions and a verbal walk-through of the recovery actions may be conducted in advance of the exercise to prepare participants for the exercise.

Test schedule

Your business recovery plan should be tested annually, with tests scheduled and monitored by the business recovery coordinator in accordance with direction from management and in concert with the recovery team leaders.

Testing can be scheduled at times less critical in the normal business cycle (i.e., not during a product launch). Testing should provide minimal disruption to normal operations and customer service and duration of each test should be estimated to ensure test participants schedule adequate time.

The business recovery coordinator, with the recovery team leader, is responsible for:

- Defining objectives to be achieved by the exercise
- Developing detailed test plans
- Setting the specific date, time and place for the exercise
- Carrying out the exercise as defined for their team
- Documenting the results of the exercise
- Developing a recommendation for further testing
- Updating the plan based on the results of the exercise

Detailed discussions and a verbal walk-through of the recovery actions may be conducted in advance of the exercise to prepare participants for the exercise. The team leaders may perform these independent of the business recovery coordinator. The walk-through will help estimate the time required to perform the exercise.

The following five-year testing program covers all recovery teams and provides a progression of exercise complexity. Specific objectives and dates will need to be established as well as the exercise scenarios for exercises.

Team Description	Year 1	Year 2	Year 3	Year 4	Year 5
Recovery management team	🟠		🔵		🟢
Operations recovery team	🟠	🟡	🔴	🟢	🔷
Information systems recovery team	🟢	🟢	🟢	🟢	🔷

Key: (see Types of Tests section for descriptions)

🟠 Recovery plan checklist	🔵 Risk assessment, BIA and recovery
🟡 Structured walk-through test	🟢 Recovery simulation
🔴 Emergency evacuation drill	🔷 Integrated recovery simulation

Other activities that need to be scheduled and carried out annually are:

- Modification of the business recovery plan based on exercise results
- Development of the testing schedule for next year
- Preparation and presentation of a report on the exercises with a proposed future exercise schedule to senior management and board of directors

Management and the business recovery coordinator should evaluate the testing program annually and adjust the program to provide for tests of those areas affected by major changes in personnel, equipment, operating software or recovery strategies.

Development of your test plan

The recovery team leaders, with guidance from the business recovery coordinator, are responsible for the development of detailed test plans. Considerations in the development of tests are:

- Objectives of the current year testing program
- Recovery objective to be tested
- Type of test
- Timing
- Scheduling
- Duration
- Test participants
- Assumptions
- Constraints
- Assignments for those assisting with the exercise
- Test steps

Various test scenarios should be planned that identify the type of disaster, the level of damage, recovery capability, staff and equipment availability, backup resource availability and time/duration of the test. When developing your test plans, you should identify the person responsible for each step and the estimated time required to perform each action.

Evaluating the test exercise

Four factors are to be evaluated following each exercise:

- The team's ability to perform the recovery procedures
- The value of the plan as an aid to the team conduct of recovery activities
- The ability to achieve recovery time objectives in simulation tests
- The conduct of the exercise

A team customer should be designated to log events and activities during the exercise to provide accurate information for the debriefing session following the exercise.

These factors are interrelated, but the evaluation process should result in identifying improvements in the team customer preparedness, the plan document and exercise administration. The recovery team customers can provide useful information to evaluate the four factors and the ability to recover from disaster situations.

A team customer should be designated to log events and activities during the exercise to provide accurate information for the debriefing session following the exercise. The feedback from the team customer evaluations, test results worksheets and debriefing sessions should be provided to the business recovery coordinator for analysis and use in updating and enhancing the plan and testing program.

Test results documentation should be completed and stored in a safe place for future reference by the business recovery coordinator, regulatory agencies or other authorized third parties. A summary of the testing and test evaluations should be presented to senior management and the board of directors.

Testing forms that you will create

- **Test preparation worksheet** – This is a worksheet that is used for planning the test exercise. Teams will use this form to list all procedures and areas of responsibility to be tested in accordance with an exercise objective. Once tested, the results of the test should be documented in your own test results worksheet.
- **Testing checklist** – This is a checklist to assure sufficient supplies, reports, and forms are available, that policies have been defined and telephone inventories are current during a checklist test. The planned test and results are documented on this single form.
- **Test results worksheet** – This is a worksheet you can create for documenting testing procedures and evaluation of the results of various tests. A record of plan modifications should be included in the documentation.

Testing procedures

Separate and combined tests should be performed at various intervals to ensure the adequacy of the business recovery plan. All testing exercise participants should be given ample notice of the scheduled test. This will allow for proper scheduling of key personnel, and provide adequate time to reschedule the test if a significant number of participants cannot participate without disrupting operations. The team leader should designate a substitute if a team customer cannot be present for a test. The organization should ensure participation in test activities is supported by senior management and given a high priority.

Procedures for conducting the four types of tests are provided below. These procedures may be altered, based on the exercise participants and the objectives.

Checklist test

Participants

- Business recovery coordinator
- Team leaders, customers and alternates
- Facilitator
- Other personnel as determined necessary

Procedures

- **Business recovery coordinator**
  - Meet with all participants to explain the purpose and scope of the test
  - Review the plan assumptions, summarize the plan and recovery strategies, review applicable sections of the plan in detail with the group and explain the recovery organization structure
  - Review disaster definitions and plan activation procedures
  - Instruct all team managers to inventory their off-site storage items to ensure all required supplies are on hand
  - Review the recovery process to be used by the team
  - Review supplemental manuals and data inventories as appropriate and provided in your testing checklist
  - Review the results of the exercise with participants and request they provide an evaluation of the exercise
  - Prepare the exercise report of participants, objectives, results, action items and recommendations for subsequent exercises, providing a copy to management

- **Team leaders**
  - Distribute the applicable sections of the plan to each team leader and alternate for their review, along with blank copies of the relevant exhibits
  - Verify copies of the plan are distributed and stored according to the distribution register
  - Review the applicable sections of the plan and gather updates from team customers
  - Lead the team customers in conducting the inventory of supplies, equipment, forms, reference materials and vital records that are to be retained off-site
  - Ensure timely feedback from various team customers on the results of the inventory and exercise
  - Maintain a file of maintenance forms that will provide evidence that the review and test have been performed

- **Team customers**
  - Review the distributed sections of the plan and identify any portions that are unclear or appear to be inaccurate
  - Provide the team leader with observations and recommendations about the plan
  - Conduct the inventory of supplies, equipment, forms, reference materials and vital records that are to be retained off-site as defined in the plan, noting any differences in terms of content, quality or version
  - Provide the team leader with the results of the inventory and with recommendations for changes in the items retained off-site
  - Provide the team leader with an evaluation of the exercise and with recommendations for future exercises

Structured Walk-Through Test

The structured walk-through test is a test usually performed with a single team. A version of the test can be performed with team leaders to exercise coordination between teams.

Participants

- Business recovery coordinator
- Team leaders, customers and alternates
- Facilitator
- Other personnel as determined necessary

Procedures

- **Facilitator**
  - Assure the plan, including exhibits, has been distributed to each participant and has been updated in advance of the exercise
  - Meet with all participants to explain the purpose and scope of the test and explain the sections of the plan to be exercised
  - Describe the disaster scenario (situation) to be used for the exercise backdrop, including:
    - + Description of the type of disaster
    - + How the situation was reported
    - + Time of day and day of month the disaster was reported
    - + Extent of damage to the involved site and anticipated period of unavailability
    - + Extent of damage to equipment, including time frame for replacement or repair
    - + Effect on facilities, surrounding geography, voice and data communications, personnel (i.e., injury or death) and other pertinent information
  - Describe the plan activation criteria and whether the plan is activated under the described circumstances

  - Request the team leader to provide direction to the team customers as they describe their responses and actions to the situation
  - Monitor the various team activities, noting the performance of the team customers to the disaster scenario
  - Provide additional events, clarifications to the situation, and simulate responses from other recovery teams, as appropriate, to keep the simulation active
  - Identify enhancements needed to the plan
  - Assemble the team customers at the completion of the structured walk-through test for a debriefing to discuss general observations, ideas, suggestions and team-specific changes or suggestions relating to the plan
  - Prepare an evaluation of the team's performance and identify enhancements to the plan and exercise
  - Meet with the team leader to discuss specific suggestions and changes that will enhance the team's preparedness, the plan and future testing
  - Assign responsibilities for updating the plan; include the date the update is to be completed, based on the team leader's feedback
  - Maintain a file of update forms to provide evidence that the review and test have been performed

- **Team leader and alternate**
  - Review the applicable sections of the plan and prepare the team customers for the exercise
  - Direct the team customers through the recovery process as dictated by the simulated disaster situation
  - Note additions, changes and deletions to the plan
  - Provide the plan maintenance form to appropriate personnel to record amendments to the plan
  - Complete the test results worksheet to help the team in documenting the tests and results
  - Return the completed forms to the person responsible for updating the plan or the to the business recovery coordinator by the due date. If no revisions were necessary, the team leader should prepare a brief memo documenting that no plan update was required
  - Prepare the exercise report, which should contain the following information:
    - List of participants
    - Date the test was performed
    - Statement that no revisions were noted during the review, if applicable
    - Team manager's signature
    - Comments, observations and enhancements

- **Team customers**
  - Review the applicable sections of the plan
  - During the walk-through session, describe the activities to be performed as documented in the plan, noting how the activity will be accomplished; who will specifically perform the task; what resources are required to accomplish the task; the estimate of time required to perform the activity or the duration in which it can be performed; whether the activity can be completed successfully
  - Complete all exhibits and worksheets relevant to the scenario
  - Participate in the post-exercise debriefing and evaluation

- **Business recovery coordinator**
  - Schedule personnel and arrange for facilities to conduct the structured walk-through test
  - Assist in documenting the activities that occur during the exercise and discussions during the debriefing
  - Participate in the post-exercise debriefing and evaluation
  - Maintain a file of update forms to provide evidence that the review and test have been performed
  - Assurance business recovery plan updates are applied and revised plans are distributed according to the distribution register

Recovery simulation

The simulation test may be performed with a single team (e.g., IT recovery team) or with several teams (e.g., IT recovery team and dependant teams). The test involves simulating the operations following a disaster situation using materials and equipment provided for at the recovery location.

Participants

- Business recovery coordinator
- Team leaders, customers and alternates
- Facilitator
- Other personnel as necessary

Procedures

- **Business continuity coordinator**
  - Schedule personnel and arrange for facilities to conduct the recovery simulation
  - Ensure availability of equipment and supplies stored off-site for recovery operations to be used during the recovery simulation
  - Assist in documenting the activities that occur during the exercise and discussions during the debriefing
  - Participate in the post-exercise debriefing and evaluation
  - Maintain a file of updated forms to provide evidence that the review and test have been performed
  - Assure business recovery plan updates are applied and revised plans are distributed according to the distribution register
- **Facilitator**
  - Assure the plan, including exhibits, has been distributed to each participant and has been updated in advance of the exercise
  - Prepare materials and scenarios to be used in staging the simulation, and arrange with the business recovery coordinator for personnel to assist in conducting the exercise
  - Meet with all participants to explain the purpose and scope of the test, explain the sections of the plan to be exercised, and detail assumptions and limitations to be applied during the exercise
  - Describe the disaster scenario (situation) to be used for the exercise backdrop, including:
    - + Description of the type of disaster
    - + How the situation was reported
    - + Time of day and day of month the disaster was reported
    - + Extent of damage to the involved site and anticipated period of unavailability
    - + Extent of damage to equipment, including time frame for replacement or repair
    - + Effect on facilities, surrounding geography, voice and data communications, personnel (i.e., injury or death) and other pertinent information
  - Describe the plan activation criteria and determine whether the plan is activated under the described circumstances
  - Dismiss the teams to their team leaders to initiate their activities for responding to the situation and recovering operations
  - Monitor the various team activities, noting the performance and understanding of their responsibilities, carrying out activities relevant to the recovery, and coordinating with personnel and teams. Identify enhancements to the plan and team preparation
  - Introduce additional challenges or situations during the simulation to which the team customers need to evaluate and respond. Coordinate "actors" who are assisting with the simulation in their delivery of situations to which the teams are expected to respond
  - Reassemble the teams following completion of the test for a debriefing to discuss general observations, ideas, suggestions and team-specific changes or suggestions

  - Evaluate the group's performance in responding to the disaster scenario, identifying enhancements to the plan and the level of team preparedness
  - Meet with the team leaders individually to discuss specific suggestions and changes that will enhance the plan and the future testing environment
  - Prepare a report on the exercise, follow-on activities and recommendations for future exercises

- **Team leader or alternate**
  - Review the applicable sections of the plan
  - Prepare the team customers for the exercise
  - Direct the team customers through the recovery process as dictated by the simulated disaster situation
  - Note additions, changes and deletions to the plan
  - Provide the plan maintenance form to appropriate personnel
  - Complete the test results worksheet to help the team document the tests and results
  - Return the completed forms to the person responsible for updating the plan or to the business recovery coordinator by the due date. If no revisions were necessary, the team leader should prepare a brief memo to the business recovery coordinator documenting that no revisions to the plan were necessary
  - Prepare the exercise report, which should contain the following information, and forward to management:
    + Exercise objectives and participants
    + Date exercise was performed
    + Activities performed
    + Degree to which the objectives were achieved
    + Statements about identified revisions to the plan or that no revisions were required
    + Recommendations to further improve preparedness
    + Comments and future exercise recommendations

- **Team customers**
  Review the applicable sections of the plan, understand the duties for recovery of operations and perform the activities described in the plan:
  - Use the equipment and supplies provided for recovery
  - Interact with the actors simulating the situations to be performed
    + Initiate and respond to communications for carrying out the recovery activities
  - Complete all exhibits and worksheets relevant to the exercise
  - Participate in the post-exercise debriefing and evaluation
  - Prepare and assist in plan updates or enhancements

Recovery simulation – information technology

This exercise requires movement of various tapes, materials, personnel, etc., to the recovery site, as well as setup of the equipment and communications necessary for alternate processing by the IT recovery team.

Participants

- Business recovery coordinator
- IT recovery team personnel, as appropriate
- Other personnel as determined necessary

Procedures

- **Business recovery coordinator**
  - Distribute the entire plan, including blank copies of all applicable exhibits, to each participant
  - Monitor the test and note changes, discussion

points and observations for later discussion with the team leaders

- Reassemble the teams following completion of the test to discuss general observations, ideas, suggestions and team-specific changes or suggestions relating to the plan
- Meet with the team leader and alternate individually to discuss specific suggestions and changes that will enhance the plan and the future testing environment
- Evaluate the group's performance in simulating the disaster scenario and identifying enhancements to the plan
- Update the plan based on the feedback from the team leader/alternate
- Maintain a file of maintenance forms that will provide evidence that the review and test have been performed
- Retain a representative sample of materials, including test results, in a file for review by regulators, third-party auditors or internal auditors

- **IT recovery team leader**
  - Develop an estimate of costs that may be incurred relating to the test and obtain management approval prior to proceeding
  - Meet with all participants to explain the purpose and scope of the test
  - Explain to the participants that backup materials and supplies may be retrieved only from the off-site storage location for this test
  - Develop a written schedule describing major activities, time frames and responsible persons for each major activity within the test
  - Track the number of hours used for testing and be cognizant of limitations and potential additional costs
  - Track expenses relating to the test and review alternatives following the test that could potentially lower expenditures
  - Lead the post-exercise discussion with team customers to review the results of the exercise and improvements to be made in the plan or exercise
  - Manage the development and publishing of changes to the IT recovery team plan
  - Prepare the post-exercise report for management and the business recovery coordinator, noting:
    - + Exercise objectives and participants
    - + Date exercise was performed
    - + Activities performed
    - + Degree to which the objectives were achieved
    - + Statements about identified revisions to the plan or that no revisions were required
    - + Recommendations to further improve preparedness
    - + Comments and future exercise recommendations
- **IT recovery team**
  - Move the necessary materials (e.g., magnetic tapes, reference manuals and supplies) from the off-site storage facility to the alternate processing site
  - Discuss the following with the team leader before starting the simulation:
    - + Notification responsibilities by various team customers
    - + Coordination responsibilities to and from the vendors
    - + Critical forms and supplies that may be needed
    - + Backup and off-site storage of production files
    - + Rotation of IT staff
  - Use the IT recovery team plan to restore the computer and communications environment
  - Consider changes in the security of operating and application systems that may be necessary to operate in an emergency mode
  - Verify the usability of the restored environment by accessing data and simulating processing

- Check the configuration of all network equipment and test communication circuits
- Note changes and enhancements that may be appropriate, and discuss these with the business recovery coordinator and team leader following the test
- Discuss staffing requirements as described in the plan
- Supplement minimum staff with temporary resources, if needed
- Prepare and assist in plan updates

Communications test

The communications test is a specialized type of simulation test that addresses the data communications recovery capability. The test can be independent or in conjunction with an IT recovery team simulation test.

Participants

- Business recovery coordinator
- IT recovery team leader/alternate
- IT recovery team customers
- Other personnel as necessary

Procedures

- **Business recovery coordinator**

  Distribute the application sections of the plan to each participant, along with blank copies of the following forms that you have created: the test preparation worksheet, the test results worksheet and the plan maintenance form.
  - Monitor the test and note changes, discussion points and observations for later discussion with the team leader
  - Meet with the team leader and alternate individually to discuss specific suggestions and changes to enhance the plan and future testing
  - Evaluate the group's performance in the recovery of communications in the disaster situation and identify plan enhancements
  - Monitor the plan update, including its date, based on the team leader feedback
  - Maintain a file of updated forms to provide evidence that the review and test have been performed

- **IT recovery team leader**
  - Develop an estimate of costs that may be incurred relating to the test and work with the business recovery coordinator to obtain management approval prior to proceeding
  - Meet with all participants to explain the purpose and scope of the test
  - Explain to the participants that backup materials and supplies may be retrieved only from the off-site storage location for this test. No items from the information technology department are to be used
  - Develop a written schedule describing major activities, time frames and persons responsible for each major activity with the test
  - Track expenses relating to the test and review alternatives following the test that could potentially lower expenditures
  - Select the remote location(s) to be used in establishing the communications environment
  - Establish criteria for determining that communication links are operational with sufficient capability to meet the recovery requirements
  - Manage the recovery efforts during the simulation, drawing on additional technical assistance as required to address situations beyond the team's capability
  - Lead the post-exercise debriefing of the team to identify the aspects of the existing strategy and plan that could be refined to reduce recovery time, cost or effort, and establish recommendations for future exercises that would further improve the recovery capability
  - Manage the development and editing of changes to the IT recovery team plan
  - Prepare post-exercise report for management and business recovery coordinator, noting:

    - + Exercise objectives and participants
    - + Date exercise was performed
    - + Activities performed
    - + Degree to which the objectives were achieved
    - + Statements about identified revisions to the plan or that no revisions were required
    - + Recommendations to further improve preparedness
    - + Comments and further exercise recommendations

- **IT recovery team**
  - Obtain backup media and reference/operating manuals from off-site storage. For those manuals not stored off-site, discuss with the team leader how to obtain copies from the appropriate vendors on an expedited basis
  - Discuss staffing requirements as described in the plan
  - Supplement minimum staff with temporary resources, if needed
  - Establish communication links between the recovery site and user recovery area
  - Perform end-to-end tests for connectivity
  - Manually dial designated test locations intended to be supported by dial backup
  - Establish voice communications with test personnel housed at alternate sites
  - Initiate monitoring of the alternate communications network
  - Note changes and enhancements that may be appropriate, and discuss these with the business recovery coordinator and team leader following the test
  - Prepare and assist in plan updates or enhancements

Summary

There's a lot to testing your business continuity plan, but hopefully this chapter has helped you understand the value of proper testing. Remember, these are not pass/fail tests; they are designed to show your command of the subject matter and reveal any weaknesses in your BC plan.

Testing will determine the reliability and compatibility of your backup facilities, verify the completeness and accuracy of your plan, identify the areas that need enhancement, give you a way to integrate plan maintenance and improvement and help you train your teams and prepare them for any eventuality. If your company ever does suffer the effects of a major disaster like the Great Chilean Earthquake of 1960, your organization stands a good chance of being one of the businesses that is able to recover quickly and get back to work with the least possible downtime.

1
2
3
4
5

ABOUT THE AUTHOR

Greg Livingston, CBCP, CDRP is a business continuity planning expert and the managing director of Conestoga Systems, LLC, a Service Disabled Veteran Owned company based in Southern California. Greg consults to various business and government entities, including regulated, non-regulated, public, private, educational, retail and government, in areas of enterprise risk management, business continuity, disaster recovery, crisis management, process management and emergency management. Throughout his more than 30 years as a risk management professional, Greg had led numerous engagements for clients in a wide variety of industries. Contact Greg at greg.livingston@conestogasystems.com.

ABOUT CONESTOGA SYSTEMS

The risk management professionals at Conestoga Systems help clients in understanding and proactively preparing for all types of business risks. Service offerings include controls consulting, audit preparation, regulatory compliance, business continuity, crisis management, emergency management, and disaster recovery planning. The firm's staff have extensive experience in business continuity planning and other related fields, hold numerous certifications (CBCP, MBCP, CPP, CISA, CCP, etc.) and have published books and articles on business continuity planning. Centurion's industry experts have also been featured speakers at numerous business continuity, technology and trade association seminars.

ABOUT ONSOLVE

OnSolve is the market leader in real-time, mass notification and collaboration solutions used by the world's largest brands and thousands of government agencies to deliver critical information in any situation.
Mass notification and collaboration is an essential element of emergency response and business continuity planning, keeping teams on track and coordinating during critical events. The OnSolve suite of critical communication tools is a key component of the business continuity, emergency response, IT alerting, employee safety and security programs of every organization we serve. Visit us on the Web at www.onsolve.com.

OnSolve
866 939 0911
onsolve.com

ONSOLVE™