Streamline Business Continuity Planning With Enterprise Content Management

A Laserfiche Executive Focus White Paper

Run Smarter®

Laserfiche®

Streamline Business Continuity Planning With Enterprise Content Management

A Laserfiche Executive Focus

White Paper

Table of Contents

Introduction

The recent ten-year anniversary of 9/11 served as a sobering reminder that disasters can change the face of business in the blink of an eye. With careful planning, however, unforeseen events do not have to derail your organization's ability to operate.

This is particularly true when it comes to your IT systems. Organizations today have more than just a server to recover. Now, there are several platforms that must be restored, ranging from mainframes and distributed processors to servers, PCs and telecommunications systems. More complicated data recovery solutions, such as data replication, mirroring, clustering and tiered storage, are required to help organizations cope with the unexpected and rapidly resume operations.

Also, organizations have begun to realize the impact of disaster. In 2008, ESG, a consultancy group focused on storage and information management, found that 63% of organizations could withstand only four hours or less of downtime before experiencing adverse effects to the business. For organizations like online merchants or online brokerage firms, this recovery window is even shorter, as the value of data has increased and corporate governance requirements have mounted.

Depending on the organization and industry, the time to get critical applications up and running after an outage has decreased from hours to minutes—or even seconds.

For organizations that rely on their IT systems as a revenue generator, not solely as a record keeper, the importance of guaranteeing uptime is crucial. For these IT systems, value is attached on a minute-by-minute basis. While losing organizational information is disastrous, losing transactional information—and its associated revenue—can be catastrophic.

With more and more small- and medium-sized businesses relying on transactional data from Web sales, POS systems, e-mail and fax archives and VOIP systems, losing access or connectivity through downtime means an extensive loss of revenue. Protecting your organization from downtime is crucial to minimizing its impact.

Business continuity planning is the solution to mitigating the impact of a disaster, no matter its source. Industry estimates show that **40% of organizations without business continuity and recovery plans will go out of business within a few years of a major disaster.** In fact, the Institute for Business and Home Safety, an insurance industry trade group, estimates that **25% of businesses that close during a disaster will not re-open.**

This white paper discusses the role an enterprise content management (ECM) solution should play in your organization's business continuity plan. Learn what disasters are and how disaster recovery and business continuity planning work in tandem to help your organization react more effectively, and discover strategies for developing a plan of your own.

Defining “Disaster”

Defining what a disaster actually is has become crucial as organizations shift their perception of disaster. When you think of a “disaster,” natural disasters like floods, fires or earthquakes immediately spring to mind. But consider:

- **A pandemic**. Recent projections show that an avian flu pandemic could potentially infect millions of people over an undefined period of time. In fact, the Congressional Budget Office estimates that in an avian flu pandemic, 30% of employees would become ill, missing an average of three weeks of work. Of those who become ill, 2.5% will die. If a large portion of your workforce is incapacitated, do you have contingency plans in place to replace missing employees?

- **A transportation strike or public transit failure**. If there is a disruption to the public transit system, whether by strike, infrastructure failure, natural disaster or an attack such as the 2005 bombing of the London Underground, it is likely that many of your employees will be physically unable to travel to work. Do you have plans for virtual offices or offsite accessibility? What about alternative transportation plans for your employees?

- **A terrorist attack**. Roughly 18,000 businesses were destroyed or displaced after the World Trade Center towers fell in 2001. Do you have a plan in place in case your office space is destroyed or otherwise uninhabitable?

Bill Long, CEO of medical billing company MultiMed, recently came face-to-face with another unanticipated threat to his business: arson.

Long recalls his first thoughts upon hearing that a three-alarm fire had nearly engulfed MultiMed’s office complex: “Of course, my first concern was my staff’s safety. But after I learned everyone was out of the building, I started thinking about what we’d need to do to get back up and running. I wasn’t in panic mode at all, thanks to of our disaster recovery plan.”

Beyond Catastrophic Disasters

It isn’t just catastrophic disasters that you need to plan for, although they do get the most attention. Even minor incidents like brownouts or freezing rain can cause network outages ranging from minutes to days, and in these cases, rapid recovery is crucial to maintaining productivity and restoring revenue generation.

A reasonable definition of a “disaster,” according to *Disaster Recovery Planning: Preparing for the Unthinkable*, is “the unplanned interruption of normal business processes resulting from the interruption of the IT infrastructure components used to support them.” This definition includes not only networks, hardware and software, but also data itself.

A recent IDG Research study showed that **92% of respondents have encountered at least one disruption to their business systems.** While high-profile events like hurricanes, earthquakes and terrorism get attention, they serve as distractions from the real threats:

- 65% report disruption from power failure.
- 65% from network outage.
- 55% from hardware failure.

Focusing on natural disasters and terrorism diverts attention from the realities of today’s business environment and the deteriorating state of IT infrastructure.

"Our major electronic workflows could halt production if they stopped working properly," says Michael Eklund, Information Systems Coordinator at RMS, a contract manufacturing company that specializes in medical device implants and surgical instruments. "Because of that, we look for reliable technology that's easy to implement, administer and use."

It is clear that the definition of "disaster" must be expanded beyond just forces of nature to everything that can impact your organization's operations, from employee absenteeism caused by an epidemic to corporate theft, vandalism and long-term unavailability of basic services. With proper planning, your organization will react with equal agility to something as commonplace as a server crash or something as seemingly unimaginable as asteroid impact.

Shift Your Perception—Disasters A to Z

Acts of war, arson, blackouts, blizzards, bomb threats, bribery, bridge collapse, brush fires, chemical accidents, civil disobedience, communications failure, cyber attack, disease, disgruntled employees, earthquakes, embezzlement, explosion, fires, floods, hardware crash, high winds, hostage situations, hurricanes, ice storms, interruption of public infrastructure services, kidnapping, labor disputes, lightning, military operations, mudslides, network failure, plane crashes, railroad accidents, sabotage, swine flu, server failure, snow storms, software failure, terrorism, theft of data, thunderstorms, tornados, transportation strike, vandalism, viruses, water damage … what else can you think of?

Lessons from Past Disasters

2005's Hurricane Katrina once again brought home the importance of comprehensive disaster recovery planning. With a cost of over $200 billion—with the greatest losses from disruption to businesses faced with damaged facilities, displaced employees and business interruption—Katrina caused organizations to face the question of whether they are truly prepared to recover quickly and continue operating after a disaster.

"9/11 and Hurricane Katrina just proved the need to be able to continue running a business or government office immediately after a crisis," says Karen Briner-Peterson, Director of Human Resources and Records Management Officer for New York's Jamestown Public Schools. "Our largest concern was that we had no disaster plan in place. If water pipes broke or a fire started, we had no ability to recreate our paper documents."

There was a surge in disaster recovery and preparedness planning after 9/11, when organizations were forced to consider how they would continue operations if their offices were uninhabitable for not just weeks, but months or years. But these plans began to gather dust as executives were lulled into complacency. Months, then years, went by without updating or testing disaster recovery plans.

When the Northeastern Blackout of 2003 hit, organizations were left with out-of-date and inadequate recovery plans. This massive power outage occurred throughout parts of the Northeastern and Midwestern United States, and Ontario, Canada on August 14, 2003, affecting approximately one-third of the population of Canada (10 million people in Ontario) and one-seventh the population of the United States (40 million people in eight states). **Outage-related financial losses were estimated at $6 billion.**

The Northeastern Blackout was a huge catalyst in the changing perception of what disaster recovery planning actually means. As a result of the 9/11 attacks, the U.S. Securities and Exchange Commission (SEC) and other government agencies had recommended that all Wall Street firms move their backup facilities from 50 miles outside of New York City to 125 miles, as well as put them on a separate power grid. The establishment of "Wall Street West" in the Poconos allowed real-time mirroring of IT systems and, during the blackout, enabled financial markets—as well as many businesses—to continue operation by failing over to their mirrored backups. Businesses that hadn't developed comprehensive business continuity plans, however, faced crippled operations and a significant loss of revenue.

The situation hasn't improved since. In a recent study conducted by the Association for Financial Professionals, only **37% of those surveyed feel their organization could handle a Katrina-like disaster.** Most telling, only 24% had tested their business continuity plans as a direct result of the hurricane, and 50% had no plans to do so.

When 2011's Hurricane Irene caused $20 billion in total economic losses, those organizations without well-tested business continuity plans suffered the most.

Specific Lessons Learned from Past Disasters

- Consider an off-site real-time mirrored failover location on a separate power grid, so that you can continue operations in the event of a power outage or natural disaster localized to your immediate area.
- Assign back-up roles in case key players are unavailable or missing.
- Plan for all possible communication issues, including use of satellite phones, hotlines and Web alerts.
- Establish accessible spending accounts for employees, make standing lodging arrangements near your recovery site and account for other logistics, like mail delivery and payroll.
- Plan for extended recoveries, in case business is displaced longer than expected.
- Keep your organization's documentation, scripts and business continuity planning handbook up to date.
- Provide an alternative method of accessing your data and documents.
- Be sure all vendor contracts are complete and up-to-date, including those with providers of media storage, insurance and fuel.
- Plan for business continuity, because no one else will do it for you.

Disaster Recovery and Business Continuity Planning: Mutually Exclusive, or Better Together?

The terms “disaster recovery planning” and “business continuity planning” are often used interchangeably, but they are two different concepts that work together as complementary components of an organization’s overall recovery and continuity planning.

Disaster recovery planning (DRP) is chiefly concerned with the recovery of systems and infrastructure components. By definition, it is limited in scope to a set of defined IT systems and infrastructure, with the ultimate goal of complete recovery within a defined timeframe and with a minimum of data loss. Because of the heavy emphasis on IT infrastructure, it may exclude non-IT business units such as accounting, marketing and sales, except in terms of software applications used by these departments. One issue with disaster recovery planning is that, because of the IT focus, incorrect assumptions may be made or subtleties or dependencies that are not hardware or application dependent—such as content management, document retention and security—may be missed.

Business continuity planning (BCP) is an attempt to blend the IT emphasis of disaster recovery planning with a larger-scope determination of which business components and functions must be prevented from interruption or, if interrupted, recovered immediately. It is an iterative process designed to identify these mission-critical functions and enact the policies, processes, plans and procedures that ensure their continuation if an unexpected event were to occur.

The exact functions covered by BCP vary by industry and may include processes that are not necessarily software applications, but also:

- Infrastructure (office space).
- Supplies (marketing materials and forms).
- Human resources.

BCP is also governed by industry-standard regulations, such as the Sarbanes-Oxley Act, HIPAA and FDIC/SEC rules and regulations, as well as “quasi-regulations”—industry standards and best practices that should also be followed—such as FEMA 141, which covers disaster recovery planning for business and industry; ISO 15489, which governs records management; and NFPA 232, which concerns the physical protection and storage of documents.

Basically, **your organization can have a working disaster recovery plan without a working business continuity plan, but not vice versa.** For organizations that have neither, the best move is to start by designing a plan that is a blend of both. For organizations that have already developed a disaster recovery plan, that knowledge can be leveraged into the creation of a business continuity plan.

The scale, cost and impact of a business continuity plan are enterprise-level and must be managed by a C-level executive. While some companies have begun creating the position of “Chief Recovery Officer,” usually the CEO or CFO manages the plan and assures buy-in from other executive-level staff.

Implementing a Business Continuity Plan

An effective business continuity plan is more than just the result of effective backups and data replication. An effective plan must not only be based on sound knowledge of your organization's culture and structure, but also on well-defined policies and procedures that make the plan a part of your daily operations, rather than something that is referred to only in the case of an emergency.

Your business continuity plan should include policies regarding:

- **Emergency response procedures**, such as reporting and tracking.
- **An executive communication plan**, with information on communicating with organizational management and other stakeholders, if applicable, as well as what your organizational response will be if key leaders are incapacitated or unavailable.
- **A public relations plan**, determining who will speak with the media.
- **Damage assessment and insurance claims processing information.**
- **An employee communication plan**. How will you communicate with your staff if mobile phone, landline and other communications networks are destroyed? How will you locate employees to share crucial information with them? Also, your organization should have a plan in place to manage critical personnel data, such as emergency contact information, user IDs and network passwords, in case systems are down or destroyed.
- **A communication plan** for clients and vendors, because you don't want to lose contact with either group, especially if operations are disabled for a period of time.
- **Banking**, especially regarding payroll and emergency cash access. This is an area that is particularly essential and challenging during a crisis, but is probably most overlooked when planning for a disaster. If you can't access funds during a crisis, your operations will grind to a halt, and disaster relief funding may not be instantly available.
- **Human resources systems that may not be immediately mission-critical**, but will become important in the weeks or months until operations are back to normal. Consider back-ups of salary information, payroll information and personnel and tax information as well.
- **A plan to handle phone calls, Website updates, e-mail and physical mail delivery.** What if your building is destroyed and there is no office to deliver mail to? How will you update your Website if your network is disabled?

When designing your organizational business continuity plan, you should consider the full dimensions of your organization's operations, including not just IT, but also business processes, staff and compliance. Of course, the plan must be updated and upgraded periodically to ensure it still reflects the realities of your organization. And finally, don't forget funding—**only 6% of IT budgets are allocated to business continuity.**

The steps and phases of business continuity planning follow logically from the determination of what risks are most likely to affect your organization, given your industry and physical location. For example, if you are on the Gulf Coast, you are more likely to be hit by a hurricane than an earthquake.

When considering risks, think outside the accepted natural disasters and don't forget to consider things like civil unrest, sudden changes in demand or hardware failure. For a complete guide to determining what disasters should be factored into your business continuity planning, please consult the first section of this white paper, "Defining Disaster."

A gap analysis of needs and capabilities will help you determine, in a high-level way, how able your organization is to meet the basic requirements of business continuity:

- Maintaining continuous business operations.
- Achieving regulatory compliance and meeting industry standards more quickly and cost-effectively.
- Integrating risk strategies to optimize resources.
- Providing data protection, privacy and security.
- Achieving and maintaining operational planning.
- Maintaining disaster readiness and preparedness.

Once you have identified your organization's particular needs and capabilities, you can design a strategy to mitigate the identified risks and integrate both business and IT objectives into the plan. The plans and procedures you design should then be tested—along with your system architecture—to assure that your business continuity strategies will have the desired effect.

As a reminder, **these plans are not static, and must be changed, evaluated, adjusted and tested on an ongoing basis.** Too many organizations do not test their plans often enough for them to be most effective during a disruption. IDG Research found that an alarming 80 percent of organizations indicated they test their disaster recovery plans annually or less often. To ensure effectiveness, you should test and reevaluate your business continuity plan frequently, employing rotating technical staff to ensure that recovery efforts are not halted if key personnel are absent.

Implementing Your Plan

Be sure to consider the following:

- Workload division
- Hardware alignment/positioning
- Storage strategy
- Data replication strategy
- Recovery and availability strategy
- Network connectivity and capacity measures
- Shared services and infrastructure components for base operating capabilities
- Virtualization alternatives
- Systems management mechanisms, command/control mechanisms, testing capabilities, physical and logical security features

Enterprise Content Management as Part of Your Organization's Business Continuity Plan

While most organizations are quick to consider their IT infrastructure when planning for a disaster, it is easy to forget paper archives. Paper is a familiar, yet extremely vulnerable, archival medium, particularly threatened by fire, flood and theft, and may be just as important as your electronic data, especially when it comes to pre-computer historical archives.

While most, if not all, electronic records are backed up in some format, paper records are often forgotten—and once they are gone, they are gone forever. Some organizations duplicate records for offsite storage in an attempt to secure their paper records, but this is both time-consuming and expensive.

The solution is enterprise content management (ECM) technology. With ECM software, a digital image of paper records is captured and preserved in unalterable format, guaranteeing its integrity. **ECM applications also manage electronic content**—ranging from Microsoft® Word®, Excel® and PowerPoint® documents to Outlook e-mails and digital audio and video files—from the same interface, providing a secure storage and recovery solution for both paper and electronic documents.

Quality ECM solutions enable you to convert both structured and unstructured content to non-proprietary TIFF and ASCII formats and store it alongside imported electronic documents, providing for long-term access and security. Easily searchable and much more space- and cost-efficient than paper archives, digital archives should become a key factor in your organization's data storage and recovery planning.

For example, Monica Baccardax, IT Project Manager for the Faculty of Medicine at Dalhousie University Medical School, explains that her team was relieved "when they realized that our ECM system serves as a backup should paper documents be destroyed."

Law firm Arenson & Zimmerman was particularly pleased to have an ECM "backup" in place when severe flooding prevented staff from working in the law firm's offices for more than four weeks. Authorized employees used the firm's ECM system to access records remotely, which was vital to producing billable work "with little disruption to business," says Legal Assistant Laurie L. Chappell.

Pulte Mortgage, meanwhile, notes that ECM plays a critical part in ensuring continuity of operations during the harsh Colorado winters. "In the past, if we heard a snowstorm was coming, we'd move all the paper loan files that were due to close to a hotel and house our processors there until the storm had passed," says CIO Gary Ives. "Giving them access to the information they need from home saves money and energy."

ECM solutions should play a part in your organization's business continuity plan by ensuring that all organizational content is properly maintained and accessible when needed. Choosing an ECM solution that combines the flexibility of mobility with the security and manageability of centralized control gives employees secure, real-time access to mission-critical information from anywhere in the world.

For example, should your CEO become stranded in a foreign country due to a national security threat, s/he will still be able to use your ECM system to access, upload and approve documents relating to your upcoming IPO using his or her laptop, iPhone or BlackBerry.

ECM solutions can also tie into your organization's other IT solutions; for example, with DVD/Blu-ray publishing, key documents will be available to your crisis team, even while your network remains down. Storing these disks offsite keeps data secure, enabling work to continue even if your offices are destroyed or your network is disabled. Best-in-class ECM solutions not only allow you to easily transfer your records to DVD or Blu-ray, but equip them with integrated viewers and search solutions, so you will be able to access your records from any computer—regardless of whether ECM software is installed.

A back-up of your information, stored securely offsite, provides a relatively easy way to secure your data. The method of storage can vary from offsite backup to a redundant, mirrored site separated by geography, drawing from separate water and power grids. Regardless of storage method, **ECM technology assures data backup and recovery while easily maintaining information offsite**.

As John Phillips, IT Systems Analyst at the Central Contra Costa Sanitary District, says, “We hope we never face an emergency that will demonstrate the benefits of having ECM, but we have to be prepared.”

Without access to your data, key steps of your business continuity plan cannot be carried out and there is little hope of recovery.

Conclusion

An effective business continuity plan must not just protect employees and physical resources, but also protect the integrity of your organizational information, especially if it is confidential, sensitive and critical to business continuity. Enterprise content management (ECM) helps you ensure data integrity, comply with government regulations, integrate risk strategies to reduce costs and scale rapidly as your organization changes.

Despite its familiarity, paper is a vulnerable archival medium. Easily damaged, easily lost and not easily replaced, it can present a sizeable obstacle to any business continuity plan concerned with the preservation of documents and records. Because these documents represent a crucial asset to most organizations, ECM has an important part to play in business continuity plans.

The Client Records Manager at an international financial services firm explains, “We're required to resume operations within 24 hours of a disaster. When we did a simulated disaster recovery, our mirrored ECM server was back up and running straight away, and everyone went to the ECM system first to recover information. Were we to experience a real disaster, life would go on, and our clients would be none the wiser.”

ECM technology enables your organization to create a centralized repository to store all vital organizational information. Effectively delivering on a continuity plan that includes ECM as one of its components will not only enhance your ability to recover from a system failure, but will also help you to better define what records are crucial to your organization and improve your overall records management strategy.

Worksheet: Creating Your Business Continuity Plan

Creating Your BCP and Internal Audit Teams

In order to test business continuity planning (BCP) and disaster recovery (DR) compliance, a team of qualified, knowledgeable internal auditors should be created, reporting to a different member of the board than the BCP team reports to. This team of internal auditors must test policies and procedures to ensure that the BCP plan and process meet the compliance requirements.

Who will be on your business continuity planning team?

Who will they report to?

Who will serve as your internal audit team?

Who will they report to?

Risk Assessment

What risks are most likely to affect your organization, given your industry and physical location?

When considering risks, think beyond the accepted natural disasters, and don't forget to consider things like civil unrest, sudden changes in demand or hardware failure.

Are key systems backed up regularly enough (and are they able to be restored quickly enough) to ensure that availability of data meets specific business, legislation and standards requirements?

□ Yes
□ No

Are key systems' availability ensured using uninterruptible power supplies (UPS), failover/hot-standby facilities or other contingency measures?

□ Yes
□ No

Is the organization able to operate effectively without key personnel?

□ Yes
□ No

Is it clear who is the "second in command" in each department?

□ Yes
□ No

Are there at least two staff members who know how to carry out each key job?

□ Yes
□ No

Is the organization able to operate effectively without key systems (not just IT systems—telecommunications systems, manual systems, etc.)?

□ Yes
□ No

Are contingency manual processes in place in case key systems fail?

Is the organization able to operate effectively without key locations?

□ Yes
□ No

Are contingency locations available in which business can temporarily be carried out if a site/location is unavailable?

____

____

____

Are all important prevention mechanisms in place to avoid or reduce the effects of system failures or damage caused by floods, fires, terrorist attacks and so forth?

Take into account firewalls, intrusion prevention/detection mechanisms, auditing/logging, sprinkler systems, closed-circuit TV cameras, security staff, physical security mechanisms (such as passcodes, keycards, receptionists, keys and locks, security fences and building design).

____

____

____

____

The risk assessment area of business continuity planning can be tested by internal auditors by obtaining a copy of the risk assessment/business impact assessment documentation, and ensuring that it covers all the required systems, locations and personnel.

Gap Analysis

A gap analysis of needs and capabilities will help you determine, in a high-level way, how able your organization is to meet the basic requirements of business continuity. This review process is the responsibility of the BCP team.

Have you had a security assessment carried out by an independent assessor (CISSP certified auditor or independent security consultancy)?

□ Yes
□ No

Have you conducted scenario testing of your BCP, such as a simulation of a terrorist bomb attack on your organization's headquarters, or simulation of a virus attack bringing down the network?

□ Yes
□ No

Changes to be made:

____

____

Have you checked to ensure that a backup plan for each key system has been implemented correctly?

□ Yes
□ No

Changes to be made:

____

____

Can backup personnel produce the backup tapes for these key systems when requested?

□ Yes
□ No

Changes to be made:

____

____

Are data restoration requirements met?

□ Yes
□ No

Changes to be made:

____

____

Are firewalls, intrusion detection/prevention systems, authentication systems (login, passwords, etc.) and logging/auditing systems operating effectively?

□ Yes
□ No

Changes to be made:

____

____

Are logs being reviewed and acted upon on a regular basis?

□ Yes
□ No

Changes to be made:

____

____

Are appropriate physical security measures in place and functioning effectively?

For example, security personnel are patrolling key areas regularly, visitors are always accompanied, security fences are in place, closed-circuit TV cameras are in place and are being watched, and security passes are required to access key areas of buildings.

☐ Yes
☐ No

Changes to be made:

____

____

Are there procedures and policies in place to prevent data integrity or availability being compromised?

For example, checks and controls ensure data integrity, and separation of duties ensures that no single person can seriously affect data integrity and/or availability.

☐ Yes
☐ No

Changes to be made:

____

____

As part of this gap analysis and review process, your BCP team should conduct regular reviews to identify any changes that should be made as a result of:

- Changes to legislation.
- Changes to the way business is carried out. (For example, a merger that adds a new business location to the plan or discontinues a business relationship with a partner, removing a location from the plan.)
- New experiences or information. (For example, many organizations have reviewed their BCP and DR plans in the light of 9/11, Hurricane Katrina, etc.)

How often will your BCP team review the plan?

____

____

____

Who will be responsible for determining when the BCP should be reviewed?

____

____

____

This review process can be tested by internal auditors in the following ways:

- Obtaining copies of the reports of any external auditors, consultants or security assessors.
- Obtaining copies of any minutes/agendas of meetings involving the BCP plan and process.
- Reviewing documentation of testing scenarios, such as test plans and test results.
- Requesting proof that any issues/problems identified were acted upon and resolved. Proof can include logs, change request documentation, printouts of software or hardware configurations, etc.
- Specifying dates for which the backup team should provide the backup tapes of all the key systems, and verifying that the backup tapes are restored effectively and correctly within data-restoration timeframes.

Business Continuity Plans, Policies and Procedures

Data recovery procedures

List your strategies to handle:

Workload division

Hardware alignment/positioning

Data storage

Data replication

Recovery and availability

Network connectivity and capacity measures

Shared services and infrastructure components for base operating capabilities

Virtualization alternatives

Systems management mechanisms

Command/control mechanisms

Testing capabilities

Physical and logical security features

Reporting

Tracking

Call Lists/Communication

It should be clear who should be called in different scenarios, and their contact details should be widely available to all who need them.

Executive Communication Plan

Who will communicate with management and other stakeholders?

What will your organizational response be if key leaders are incapacitated or unavailable?

Employee Communication Plan

How will you communicate with your staff if mobile phone, landline and other communications networks are destroyed?

How will you locate employees to share crucial information with them?

How will you manage critical personnel data, such as emergency contact information, user IDs and network passwords, if systems are down or destroyed?

Client and Vendor Communication Plan

How will you communicate with your clients?

How will you communicate with your vendors?

The internal audit team can test this requirement by requesting a copy of the latest call list and calling the people on the list to ensure that the telephone numbers are up to date and that the people listed know what to do in various scenarios. It's useful to keep a copy of the call list, and a log of the results of calling the numbers, for use by the external auditors, who will later use this evidence to ensure compliance.

Public relations plan

Who will speak with the media?

Damage assessment and insurance claims processing information

Who will be in charge of contacting insurance agents?

Where will the information be stored? How will it be accessed?

Other Procedures

Banking Emergency Procedures

How will you handle payroll?

What if you need emergency access to cash?

Human Resources Systems

These systems may not be immediately mission-critical, but will become important in the weeks or months until operations are back to normal.

How will you back up salary information, payroll information and personnel/tax information?

Phone, Web and Mail

What if your building is destroyed and there is no office to deliver mail to?

How will you update your Website if your network is disabled?

____

____

____

How will you handle incoming phone calls?

____

____

____

Ongoing Auditing

Business continuity should be an ongoing process, concerned with the development of strategies, policies and plans that will provide protection of existing modes of operating within the organization, or will provide alternative means of carrying out that organization's business in the event of disruption that might otherwise result in loss to the organization.

This aspect can be tested by the internal auditors by asking the BCP team for the following:

- Proof of regular meetings: minutes, agendas, notes, presentation slides, etc.
- Regular scenario test runs, such as test plans and test results.
- Evidence of recent change management (such as logs showing ongoing changes) and reviews to the BCP plan (for example, version history of the BCP plan and associated documents).

How frequently will your audit team test your business continuity procedures?

____

____

Information derived from "Corporate Governance, Business Continuity Planning and Disaster Recovery" by Michelle Sollicito, retrieved from **http://www.informit.com/articles/article.aspx?p=427373&seqNum=3**.

Laserfiche®

The Laserfiche Institute teaches staff, resellers, and current and prospective clients how to use Laserfiche most effectively. As part of this mission, the Institute conducts more than 500 Webinars each year, covering a variety of topics. The Institute also hosts an annual conference where members of the Laserfiche community attend presentations and network to share ideas and learn best practices. Additionally, the Institute conducts a number of regional training sessions and provides resellers with content for more than 100 user conferences each year.

The Institute also develops and distributes educational material through the Laserfiche Support Site. On this Website, clients can access training videos, participate in online forums and download technical papers and presentations that help them become savvier ECM users.

For more information, contact:
info@laserfiche.com

Laserfiche
3545 Long Beach Blvd.
Long Beach, CA 90807
United States

Phone: 562-988-1688
Toll-free: 800-985-8533 (within the U.S.)
Fax: 562-988-1886
Web: **www.laserfiche.com**

Laserfiche
3545 Long Beach Blvd.
Long Beach, CA 90807 USA
www.laserfiche.com