



Business Continuity Planning IT Survival Guide





Introduction

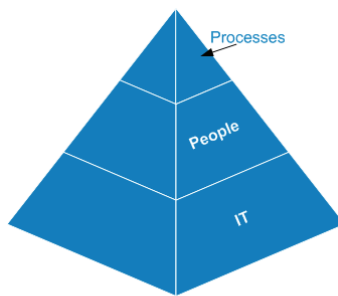
The purpose of this primer is to help businesses of all sizes begin the process of developing an effective business continuity plan designed to minimize the impact of disasters and reduce risk. To aid your planning, you will find the following:

- A definition of what a disaster is, the varying types and the effects that each may have on your business
- Suggestions on how to focus your planning efforts to meet the challenges of each disaster type
- Steps to help you begin the DR planning process to be effective
- An example of the type of information each employee should have readily available to be effective during and after the disaster

What does a disaster really look like?

The word, *disaster* often conjures negative Hollywood images — fiery explosions, great floods or buildings lying in ruins before the credits roll. But the truth is, disasters are anything that can cause a disruption in your business. They come in various shapes and sizes, have broad or narrow scopes, and are far more likely to happen than you may think, such as:

- Regional events such as fires, earthquakes, or storms that close your primary offices, temporarily or permanently
- Local events like a bulldozer accidentally cutting electrical or data line that partially or completely shut down your data center
- Company-specific events such as ceiling tiles falling due to water leaks
- System-specific events such as employee errors or software bugs that erase 6 months of data or take down an entire system



Protecting core processes includes the people and IT tools required to support them

It used to be enough to make copies of critical data files on floppy disk but today, IT has grown so complex, simply having copies of data doesn't go far enough. You need to make sure the business itself is protected, but how can you do that when there are so many types of potential disasters? Where do you start when it's impossible to think of every possible contingency?

By focusing on your business, not on the disaster. Every business consists of a set of core processes used by people in specific roles, who require certain IT systems and data. As the diagram shows, when you know what critical processes to protect, the people and IT systems required to support those processes become easier to identify and cover in DR plans.

Focusing on the business instead of merely on the disaster helps to ensure your business can survive the challenges you never considered.

Key Points

- A *disaster* is any event that is capable of disrupting your business or just portions of it for any period of time
- Disaster can strike anytime, anywhere

Business Continuity Planning

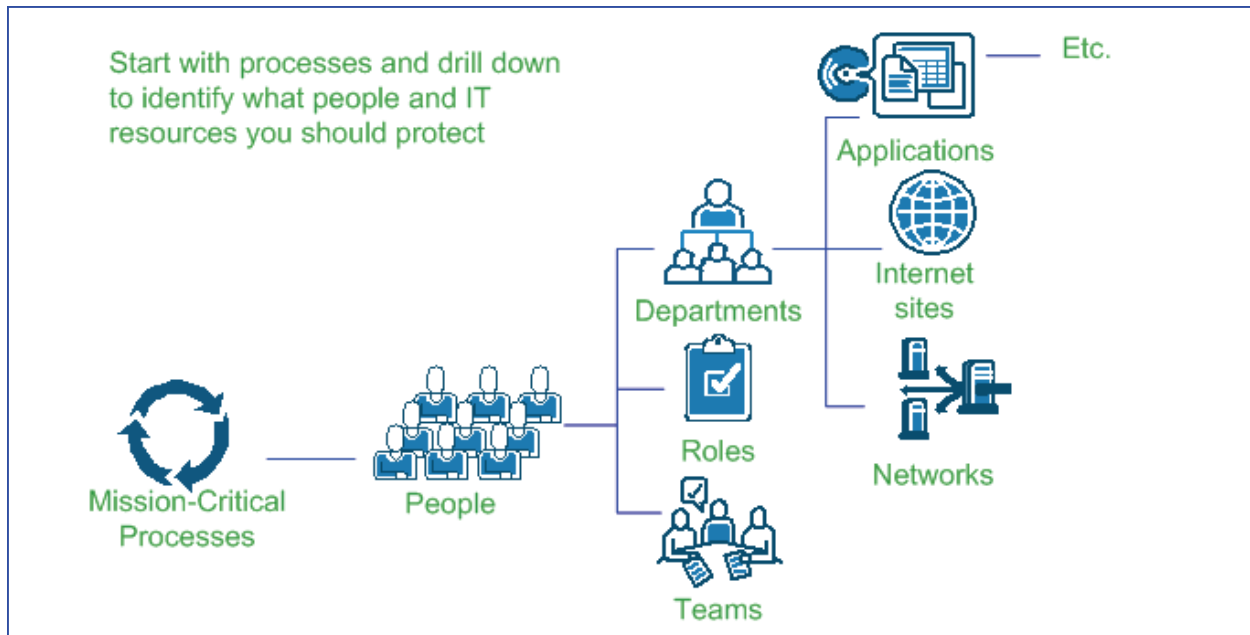
IT Survival Guide

Are you sure your mission-critical business processes are protected?

Whether your business is a one-man operation or it employs a thousand people, the starting point is the same: identify the processes critical to your success. To do this, you should first define what *critical* means in your business. Rank each process according to that definition, and then ask how long can your business survive without it, who performs it, and what IT resources support it. Questions you can ask:

- Can you simply not survive without this process? This should be your primary priority. Your business continuity plan must protect all primary priorities when a disaster strikes.
- Can you survive only a day or two without it? This should be a secondary priority. Your business continuity plan should address all secondary priorities after primary priorities are handled.
- Can you survive a week or more without it? Add it to your list of low priorities.

Suppose your call center is a critical process. Your analysis tells you that thirty people in one office using six applications running on four servers, all located in the same facility, are required to keep the call center operational. The servers are already protected by standby servers at a remote location and can easily be switched over. You should now consider whether you transport thirty employees to the remote location, allow them to work from home or appoint interim employees to take over. This question can be decided based on information in the next factor in Business Continuity Planning — Threat Analysis.



Key Points

- A *business process* is more than just IT
- Focus on the processes crucial to operating successfully so you can protect the people who perform them and the IT systems and applications needed to run them



Analyze Threats

Emergencies vary widely in more than duration. As you design your plan, consider the probability of threats that are:

- **Chronicled** — events that *have* occurred (Power outages, earthquakes, hurricanes)
- **Human** — events likely from carelessness, malicious intent, fatigue, or lack of training
- **Geographical** — events likely as a result of the location of your business (floods, storms, lightning strikes, earthquakes, typhoons, tsunamis)
- **Localized** — events due to system malfunctions (assembly line failures, computer crashes, sprinkler activations, chemical spills)
- **Planned** — scheduled events (software upgrades, system tests) that go awry

Appoint a Crisis Management Team

In the call center example, who declares the power outage to be an emergency? No plan is effective if your people don't know who's in charge. You should consider empowering all employees to recognize emergencies and give them a single contact to notify so that the appropriate Response (see next section) can be activated. Who should an employee call if there is a fire, a flood, a bomb threat? Appoint a team consisting of key leaders with decision-making authority from each physical facility and/or department in your organization.

Develop a Dynamic Plan

A business disruption has a life cycle; that is, it starts small and could potentially become a disaster of epic proportion, depending on its duration. The longer the duration, the greater the disruption to your business. Your organization's response should shift as an incident evolves from *threat* to *emergency* to *crisis* to *disaster*. It's one thing to say access to contract data isn't essential for a day or two, but what about a week or two? This is why it's important to protect more than just data. Now that you know what processes are critical to the operation of your business, you can consider threats according to their impact on those critical processes. To help you mitigate impact to your core processes, your plan should address three key phases:

1. **Business Continuity Response** — these are the steps you take immediately to sustain your core processes, your primary business priorities
2. **Disaster Recovery Response** — these are the steps you take to extend your core processes indefinitely and address your secondary priorities
3. **Restoration Planning Response** — these are the steps you take to restore your business to its pre-incident level

Using the call center example, suppose the business interruption began as a simple power outage. An emergency was declared and your plan calls for a system cutover per your agreed-upon SLA with your contracted telephone company to the standby site, which is to be operated temporarily by interim employees you have previously identified and trained from less critical business processes. If the power outage is repaired within minutes or hours, your Business Continuity Response may be the only re-

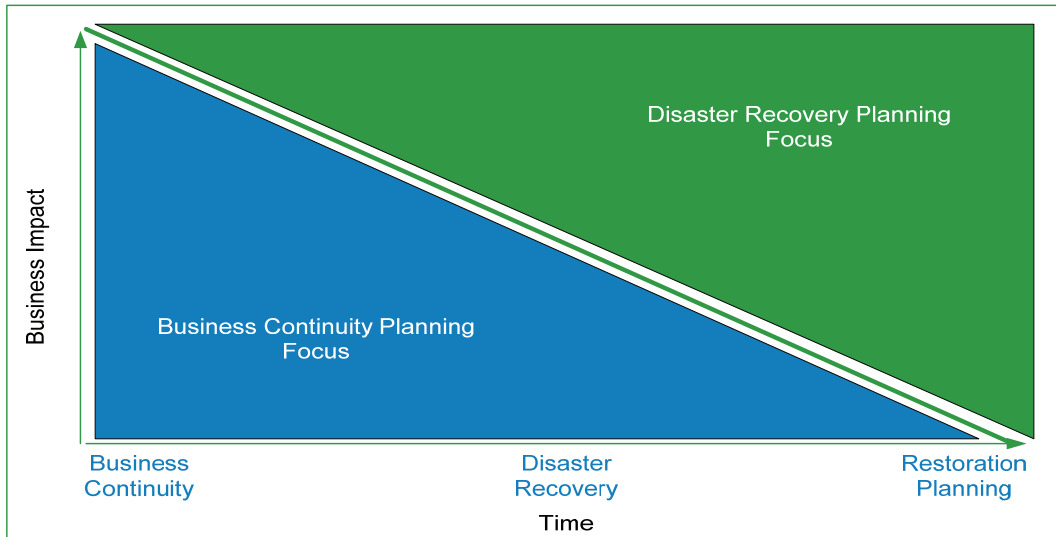
Key Points

- Align threats by probability to help you plan for likely disruptions
- Disruptions have a life cycle; consider duration when protecting key business processes

Business Continuity Planning

IT Survival Guide

sponse you'll need to make. But suppose the power outage is actually a regional black-out and local authorities cannot provide an ETA for power restoration. Your plan can now shift to Disaster Recovery Response. To sustain call center operation, you now need to fully staff the standby site so that interim employees can return to their jobs. This could include transporting employees to the standby site or hiring temporary staff. In addition, you need to bring secondary systems online, such as email or telephones.



Implement the third phase, Restoration Planning Response, if it becomes clear that the call center's original facility may never be usable. At this point, your plan should address long-term issues such as employee relocation, insurance claims, reconstruction, equipment replacement, real estate department or company for temporary location and so on.

With a phased plan, all events are considered according to business impact so that you don't need to imagine every possible threat. It makes little difference whether the call center was temporarily shut down due to a power outage or a hurricane, or permanently shut down due to a fire. What matters is you took the steps appropriate for sustaining this core function throughout the crisis. Instead of trying to create a plan for *each* threat, your goal is to create one dynamic plan that can be adjusted to any threat.

See the Case Studies for examples of Dynamic Business Continuity Plans.

Prove the Plan's Effectiveness

You already conduct evacuation drills. As part of the training process, you should conduct regular business continuity drills, as well. Include roles and responsibilities for interim employees. Train/test employees on communication procedures. Include the business continuity plan in new employee orientations. Make it part of your company culture.

Key Points

- A Dynamic Plan lets you manage any disruption according to its potential impact to your business
- Implementing a Dynamic Plan can be done in phases by business impact



What is IT's role in Business Continuity Planning?

It's true that Business Continuity Planning is about more than the IT components. Though the CEO and executive staff must define what business processes need protection and the appropriate response, IT has several innate characteristics that make them well suited to disaster planning and implementation.

- **Project planning:** IT is accustomed to implementing new technology in a controlled fashion, giving IT staff experience in understanding and planning for the impact of change for maximum success.
- **People/Process/technology relationship understanding:** Two areas in which having an understanding of this relationship are key to success:
 - The implementation of new technology often changes process. Changes in process change the ways people interact with information systems. From advanced computers and applications to systems that allow physical building access, IT understands the people/process/technology relationship better than any other team in the company.
 - IT also has a deep understanding of how supporting systems are critical to the delivery of, and access to primary information systems. From Active Directory and DHCP to routers and firewalls, IT understands the key systems and the order in which they must be restored to deliver a complete service. This understanding facilitates business continuity and restoration.
- **Experienced in disaster management:** In complex IT environments, something is usually broken or has a problem. IT has the experience to quickly identify the problem, understand the impact and respond appropriately to the issue. This experience is vital in the high stress and dynamic environment of managing a disaster event.

Do your employees know what to do when disaster strikes?

Protecting the people who work for you is as important as protecting the processes and data in your company. That protection can be as complex as offering shelter to displaced employees and their families, or as simple as identifying interim employees to perform key processes in place of the people who usually do so. Your plan should consider covering:

- Scripts, step lists or cue cards so employees can perform critical tasks and communicate with customers up to established standards
- Cutover practice drills to uncover gaps in your plan as well as rehearse procedures
- Central communication points for disseminating further instructions

Understand that disasters that interrupt your business are very likely to create stress and panic for your employees. Training employees for business continuity should also consider methods of addressing concerns and allaying fears.

Key Points

- Good communication and practice are critical for success
- Having redundant systems and backups still won't protect your business if people don't know how to access them

Business Continuity Planning

IT Survival Guide

Case Study 1— Single Site Business

Your design consulting business employs thirty people and is housed in a single leased office in a major city. During the morning rush, a large truck careens out of control and strikes the building, damaging it structurally. The building is not safe and will not be inhabitable until structural repairs are completed. You declare the emergency and activate your Crisis Management Team.

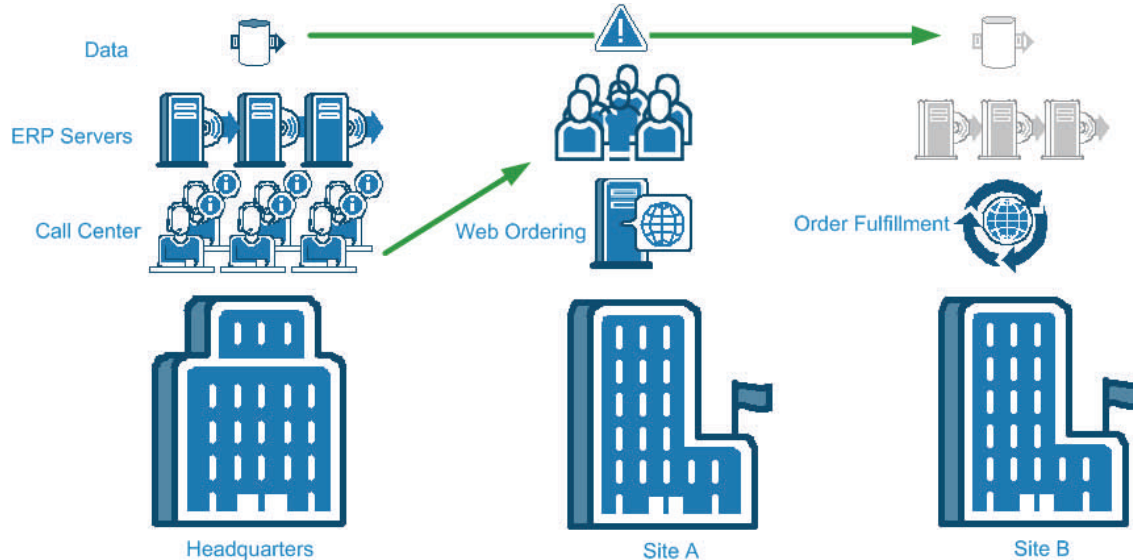
- You decide to first contact employees and have them remain at or return to home. Your emergency contact list is stored in your cell phone. You call the first contact who will initiate the phone tree portion of your communication plan. Your voice mail system is operational; your employees have been trained to check voice mail for emergency updates.
- Your next call is to the nearest hotel, with whom you've made special arrangements to provide temporary workspace, including telephone and network connectivity. With voice mail, critical employees are directed to report to the hotel site the next day and to work from home today, if so equipped.
- Next, you contact your online managed service provider, a third party partner who provides your business with data backup and replication services. Your primary business function is mission-critical—without access to your CAD drawing, email, database, and billing applications, your business fails. A managed service provider gives your business the redundant process protection you need without having to purchase equipment and resources. They can cut over to standby servers immediately.
- Key employees begin contacting customers, vendors, alarm monitoring service providers, alerting them of the crisis, as outlined by your communication plan. Your plan names a media representative who is authorized to speak with the press about the status of your business throughout the crisis. Calls are forwarded to the hotel site.
- With key processes now supported from your managed service provider and employees with laptops able to log on from the hotel, alternate or home locations, your business is able to service customers. The Disaster phase is implemented, which brings secondary processes back on line. However, a backlog of work is growing due to a lack of CAD equipment.
- Based on initial assessments, your building will not be accessible for an indefinite period of time, so you move to the Restoration Planning phase of your plan, which includes securing a new site, equipping it with powerful CAD systems and retaking control of operations from the managed service provider.
- Once the new site is secured and your business is again operating to its pre-incident levels, you improve your plan based on your experiences.

Key Points

- You identified the key processes essential for your business to survive and protected them to established service levels
- You effectively managed an unlikely event because your plan focused on protecting core business services



Case Study 2 — Multi-Site Business



Your business has three facilities located several hundred miles apart. At your headquarters, a twenty-person call center processes call-based orders using an ERP system running on three servers, also located at Headquarters. Additionally, a web-based ordering system is running at Site A and all orders are fulfilled at Site B. All three of these functions have been classified mission-critical in your Business Continuity Plan.

- An earthquake strikes the region in which your Headquarters is located. The building is slightly damaged but all employees are safely evacuated.
- The senior member of the Crisis Management Team located at Headquarters declares an emergency, activating your phase one (Business Continuity) response.
- Since earthquakes are common in this region, you have planned for this contingency. Redundant systems capable of immediate cutover were set up at Site B and staff from Site A can temporarily manage call volume switched from HQ. (See green arrows.)
- The area surrounding headquarters is heavily damaged. Employees are worried about family and property and are sent home. Your plan also activated employee assistance programs to help them handle fears and distress.
- Your Business Continuity response team initiated the crisis communication center, from which all official information is to be relayed to your employees. Training and practice drills have been conducted. Key employees are asked to report to Site A or B, as needed.
- Equipment damage is heavy. A significant portion of corporate desktop and laptop computers was

Key Points

- You identified your mission-critical processes
- You identified the IT resources required to deliver core processes and established desired levels of protection against disaster
- You trained and tested employees on their roles at and throughout the crisis
- You defined a set of responses appropriate to the business impact of interruption

Business Continuity Planning

IT Survival Guide

lost. Previously, a virtual desktop server was set up at Site B containing all required business applications, access to critical data and appropriate security software so that employees with home computers can remotely connect to Corporate IT systems and work in a safe environment that will not damage or modify their home computer systems.

- Headquarters is not safe for use according to local authorities. Repairs can be made, but are estimated to take at least two months. Your Crisis Management Team decides to move from Business Continuity to the Disaster Recovery Response phase of your plan.
- In this second phase, focus shifts to sustaining core business processes for an indefinite period of time, while bringing some secondary processes back on-line. Accordingly, your critical staff must be relocated on a semi-permanent basis to Site A, allowing the interim staff to focus on their own job functions. Instructions are relayed via the crisis communication center.
- Employees who are displaced can obtain temporary relocation assistance, if desired, according to your plan.
- Your Disaster Recovery Team puts into action the next phase of the DR plan, in which the need for restoring all secondary and tertiary processes becomes the focus.
- The Disaster Recovery Team contacts a local real-estate partner who keeps on file all vacant business locations available immediately for rent. The partner had previously kept the locations prioritized by order of environmental suitability, as had been documented for your business. They immediately identify a location that already has the required levels of telecom, power, water and physical access control. It also comes with a small datacenter room already equipped with a raised floor, internet access points and required cooling.
- The DR Team then organizes temporary furniture, telephones, computer systems, internet access, and so on.
- The Restoration Planning phase is activated when the Crisis Management team is notified that Headquarters can at last be reopened. Replacement equipment is purchased, insurance claims are filed. Employees return to work. Systems and networks are switched back. Your team holds a post-crisis review to adjust the plan where needed.

Key Points

- You appointed a Crisis Management Team empowered to make immediate decisions
- You established a crisis communication center to relay information
- You addressed employee distress throughout the crisis
- You conducted a post-crisis review of your plan to identify what worked, what didn't, and revise the plan accordingly



Sample Emergency Planning Information Checklist (EPIC)

The purpose of this sample EPIC is to help consolidate the steps you may want to consider when creating a comprehensive Disaster Recovery and Business Continuity Plan that focuses on your business goals. This checklist is just a guide. Adjust it according to your business needs.

1. Crisis Management Team (CMT)

- Identify the owner responsible for documenting and ensuring the plan's success
- Business Stakeholder Team: Identify the stakeholders in defining the plan (For example, C-level executives, department heads)
- Disaster Team: Identify the people responsible for determining the level of disaster and the required response level, who are authorized to initiate predefined actions
- Establish an emergency response hierarchy empowered to act and communicate when primary personnel are not available.

Example: Level 1 Threats

- Primary Owner: CIO _____
 - Office Phone
 - Cell Phone
 - Home Phone
 - If no response after 10 minutes, alert Secondary Owner
- Secondary Owner: CFO _____
 - Office Phone
 - Cell Phone
 - Home Phone
 - If no response after 10 minutes, alert Tertiary Owner
- Tertiary Owner: Network & Systems Administrator _____
 - Office Phone
 - Cell Phone
 - Home Phone
- Response Management Team: Determine who can change the plan's event responses during or after the crisis and for what purpose

2. Determine and Define Threats

- Determine threat probability for your area and business type
- Determine threat attributes
- Define and Categorize threats in to logical groups and prioritize them by severity
Threat Level Examples: (Use your own names and definitions as appropriate)
- Threat Level 1 - Regional**: Hurricane, regional flood, earthquake, tsunami, etc.
Attributes:
 - Affects entire region
 - Staff focused on family safety and health first, business functions are a focus some period after the threat is over.
 - Staff not likely to come to work and no access to physical business facilities
 - No local or remote IT system connectivity

Business Continuity Planning

IT Survival Guide

- **Threat Level 2 – Building Localized:** Fire, building damage, power outage, building flood (i.e. broken building water pipe), chemical spills, ceiling caved in, etc.
Attributes:
 - Affects building in which the business is located
 - Business functions are a staff focus after the immediate threat is over
 - Staff likely to come to work location however there is no access to physical business facilities
 - No local or remote IT system connectivity
- **Threat Level 3 – Business Type: Internal / External Network Failure:** Internet outage, complete internal network outage, etc.
Attributes:
 - Affects all primary business systems and processes
 - Business functions are a staff focus during and after the threat event
 - Staff at work location
 - No local or remote IT system connectivity
- **Threat Level 4 – Business Type: System or Data Damage:** Hard disk failure, limited network failure, viruses, Trojans, corrupted data, deleted or missing data, etc.
Attributes:
 - Affects one or more business stems
 - Business functions are a staff focus during and after the threat event
 - Staff at work but not able immediately utilize one or more IT systems or business processes
 - Local and remote IT system connectivity available
- **Threat Level 5 – Business Type: Physical Access Limitation:** Building access physically blocked
Attributes:
 - Affects building in which the business is located
 - Business functions are a staff focus during and after the threat event
 - Staff comes to work location but not able to gain access to facilities
 - No local IT system access, remote connectivity available

3. Identify, categorize key business processes

- List the processes that support your business
- Define availability requirements
- Categorize processes into logical groups and prioritize them by business importance, as determined by senior leaders

Examples: (Use your own names and definitions as appropriate)

- **Critical:** Required availability — business process must be available at all times with no or only momentary loss (Customer Support, Sales, internal and external communication, service availability, dispatch, and so on)
- **Key:** Required availability — business process must be available within 24-48 hours (warehousing, inventory, product shipping, IT helpdesk, and so on)
- **Important:** Required availability — business process must be available within 7 days (HR, Legal systems and so on)
- **Supporting:** Required availability — business process must be available within 30 days (historical document repository)



4. Identify supporting staff, applications and IT services for each key process

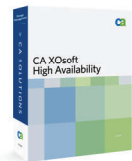
- Focus on your critical processes and complete the remaining EPIC steps. Once complete, repeat for each group of processes, completing EPIC steps a tier at a time
- Identify and list the key staff members for each process, as determined by the process owner or department head (Departments, Teams, Staff Members-secondary or backup staff members if the primary contact is not available)
- Document staff member roles and responsibilities
- Identify and list communication plan for each person (Office Number, Home Phone, Cell Phone)
- Identify the IT services required by each staff to accomplish the tasks in the process (email, CRM, Sales Accounting, Inventory, and so on)
- Document the communication services required by the staff (telephone, IM, email, interoffice mail, fax, package delivery)
- Identify the primary and supporting IT components, as identified by IT staff (servers, networks, internet access points, DNS, Active Directory, DHCP, and so on)

5. Create Response Plans

- Determine DR response levels appropriate for your business type
- Determine DR response level requirements
- Categorize capabilities and response level attributes and prioritize them according to business process availability

Examples: (Use your own names and definitions as appropriate)

- *Platinum*



- Business applications and data are protected at the highest level using application high availability with failover to either a company-owned disaster recovery site or online DR Software-as-a-Service (SaaS) provider with a 10 minute or less acceptable outage time. Each completed transaction must be protected the instant it is created.
- Business services such as telecomm have system redundancy for high availability.
- Business-critical staff have been issued portable/laptop computers for remote use. All other staff not required.
- Use *CA XOssoft High Availability* to keep all data up-to-date and provide application high availability via automatic failover.

- *Gold*



- Business applications and data are protected at the highest level using replication to a company-owned DR site or online SaaS provider with an 8-hour or less acceptable outage time.
- Business services such as telecomm have an 8-hour acceptable outage time.
- A secondary site with phones, computer systems, tables and food will be available for business critical staff. All other staff has remote access from home computer systems.
- Use *CA XOssoft Replication* to keep all data up-to-date and provide push-button failover.

Business Continuity Planning

IT Survival Guide

• Silver



- Business applications and data are protected at the daily level using backup to disk technology to an on-premise system with a 24-hour or less acceptable outage time.
- Business services such as telecomm have a 24-hour acceptable outage time.
- A secondary site for communication is available. All staff has remote system access from home computer systems.
- Use *CA ARCserve Backup* for back up to disk capability (Disk2Disk) to provide high-speed data restoration.

• Bronze



- Business applications and data are protected at the weekly level using backup to disk or tape to an on-premise system with the backup data going offsite for protection.
- Business services with outage times of 7 business days or less.
- Office is available.
- Use *CA ARCserve Backup* for back up to tape ability (Disk2Disk2Tape) to provide off-site, long term data storage capabilities with quick restore speeds.

6. The Disaster Recovery Plan

- Align the defined Threat Levels, Business Process Categories and Response Actions to meet your business needs
- Balance risks against costs



CA Instant Recovery
on Demand

- Examine hard and soft costs of supporting each business process in the identified disaster recovery level
- Is the cost worth the business risk?
- Can some of the availability requirements be realigned to meet the available funding and still meet business needs?
- Use *CA Instant Recovery on Demand* service for critical systems to provide application high availability to an off-site location while reducing your capital investment.

7. The Dynamic Disaster Recovery Plan

- Identify what would cause a change in the plan
 - What happens if the plan fails? (What if the truck carrying the backup tapes gets into an accident and cannot return with required data in time? What if the tapes are lost or can't be read?)
 - Who can determine and define plan changes?
 - Who implements changes to the plan? (Create a pool of non-business critical staff who can be used to implement ad hoc plans. Who can drive a car, bus or truck? Who can have a corporate credit card to buy needed office supplies and food?)

8. Additional Disaster Recovery Supporting Services

- What other services are only needed during a DR event that should be considered and planned for? (Rumor control, media contacts, medical services, transportation, and employee counseling)



9. Inform and train employees

- Provide updates to your employees. If they are not accessible, they are of no value.
 - Put critical information on wallet cards, binders to be taken home, send updates to PDAs and smart phones.
 - Set up phone trees for communication

10. Test, revise, test again

- Your DR plan is only as good as your last test.
- When and how often do you test your plan? How many were announced tests? How many were unannounced tests?
- How often does your business go through this complete process and make updates? Testing is more than just IT; test processes and people, too
- Test the quality of your off-site data. Bring in random tapes and see if data can be restored.
- Use *CA XOsoft Assured Recovery Option* to test your application high availability and replication environments without impacting your production environment or your protection levels.
- Conduct post-mortem reviews to ensure your DR plan keeps pace with your changing business needs.

About CA XOsoft High Availability and CA XOsoft Replication

CA XOsoft™ High Availability and *CA XOsoft Replication* are robust business continuity and disaster recovery solutions that integrate replication, continuous data protection (CDP) and automated failover for the protection of business-critical applications. Market leading features such as automated disaster recovery testing with *CA XOsoft™ Assured Recovery™* option helps you ensure successful recovery during unavoidable disasters.

About CA ARCserve Backup

CA ARCserve Backup® delivers one of the most comprehensive data protection available today. It provides centralized control and advanced features designed to address your changing business needs. This high performance solution combines innovative "D2D2T" (disk-to-disk-to tape) backup with powerful, integrated anti-virus and encryption tools, making it one of the most secure "out-of-the-box" backup solutions offered.

About CA Instant Recovery on Demand

CA Instant Recovery on Demand is a business continuity and disaster recovery managed service solution for the protection of business-critical applications. It includes all hardware, software, DR facilities and staff so there are no capital expenses. Market-leading features such as automated failover and disaster recovery testing helps you ensure business continuity in case of unplanned outages and disasters.

For more information

- To learn more about CA's industry-leading backup, business continuity, and disaster recovery products, please go to arcserve.com/products.

Business Continuity Planning

IT Survival Guide

Sample EPIC Employee Response Card

The purpose of this document is to provide information to all employees for dealing effectively with a crisis.

Incident Response Hotline (555) 555-5555

Report Incidents

Fire: (In case of fire, provide instructions here) _____

If you hear a fire alarm:

If in imminent danger: _____

If not in imminent danger: _____

Medical: (In case of medical emergency, provide instructions here) _____

Incident: (In case of other incidents, provide instructions here) _____

Regional Disasters

(Provide appropriate examples and instructions here) _____

Evacuations

If you are ordered to evacuate: _____

Congregation Point Address:

Place detailed map showing congregation point here



Media Contacts

If contacted by the media: _____

Important Contact Numbers:

Copyright © 2008 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

THIS DOCUMENT IS FOR YOUR INFORMATIONAL PURPOSES ONLY. The information contained herein may not apply to all customer situations. CA assumes no responsibility for the accuracy or the completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will CA be liable for any loss or damage, direct or indirect, in connection with this document, including without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if CA is expressly advised of the possibility of such damages.