كلية علوم الحاسب و المعلومات
College of Computer and Information Sciences

IS 414T: DISASTER RECOVERY MANAGEMENT

LECTURE 3

Information Systems Department

BCDR Plan Development

Objectives

- □ To understand the phases of BCDR
- □ To describe the BCDR Team / Personnel
- □ To describe task and resources
- □ To discuss communication plan
- □ To describe Event Logs & Change Control

PHASES OF BCDR

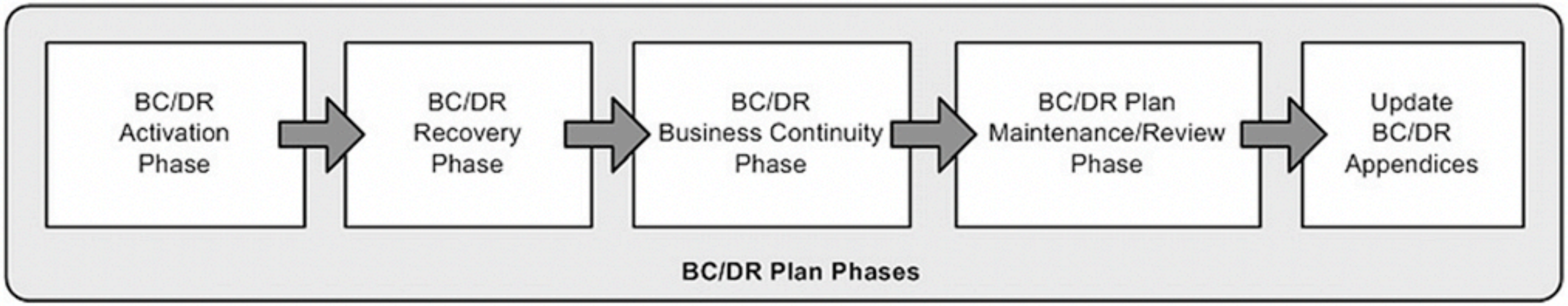

FIGURE 7.3

Phases of business continuity and disaster recovery.

Activation Phase

- □ The activation phase of your BC/DR plan addresses the time during and immediately after a business disruption.
- □ In this section of your plan, you need to define when your BC/DR plan will be activated and in what manner.
- □ You don't want to activate your plan for every little glitch your business runs into, so you'll need to develop a clear set of parameters that you can use to determine if or when to activate your BC/DR plan.

Activation Phase

- In addition, you will need to define how your plan is activated, including who has the authority to activate it, and what steps that person (or persons) will take to initiate BC/DR activities.
- Activation includes initial response and notification, problem assessment and escalation, disaster declaration, and plan implementation.
- After you have begun implementing the plan, you proceed into the recovery phase.

Activation Phase

- The plan activation phase should define various disaster or disruption levels so that you know when, if, and how to implement your plan.
- For example, if you experience a network security breach, you'll have to activate different phases of your plan than if the server room is flooded.

Activation Phase

- Let’s take a look at activating your plan for minor, intermediate, and major disasters, in that order.
- The steps you take for a minor disruption will likely be very different than the steps you take for a major disruption, so it’s important to put detail around each of these types or levels of disruption.

Minor disaster or disruption

- □ Minor disruptions occur every day in the business world and rarely, if ever, are full BC/DR plans activated.
- □ The likelihood of a minor event occurring is high, but the associated disruption is relatively low.

Minor disaster or disruption

- Here are four guidelines for defining this category.
  - Typically, the effects are isolated to one component, one system, one business function, or just one segment of a critical business function.
  - Normal operations can often continue, almost uninterrupted, in the face of a minor disruption.
  - Critical business functions still occur for some period of time after this type of disruption.
  - The failure of a single system or service can typically be addressed during the normal course of business.

Minor disaster or disruption

- For example, the failure of a single server, system disk, or phone system is problematic but usually does not require the activation of a BC/DR plan.
- There may be examples, however, where minor disruptions should be addressed by the activation of part of a BC/DR plan.
- If that is the case, be sure to clearly identify those disruptions along with which sections of the BC/DR plan should be implemented when and by whom.

Intermediate disaster or disruption

- An intermediate disaster is likely to occur more frequently than a major disaster, but obviously less frequently than a minor disaster (hence the “intermediate” designation).
- Its impact will also fall in the middle of the spectrum.

Intermediate disaster or disruption

- These are the guidelines for defining this type of disruption:
  - This type of disruption or disaster interrupts or impacts one or more mission-critical functions or business units, but not all of them.
  - Operations will experience significant disruption; entire systems or multiple systems may fail or be unavailable, but not all of them.
  - An intermediate event could include a fire or flood in the building that impacts IT systems and equipment, structural damage to part of the building where critical operations occur or where vital equipment is located.
  - An intermediate event could also include an event with a limited impact but a long duration, such as a minor disaster where recovery exceeds the established RTO.

Major disaster or disruption

- The possibility or likelihood of this type of disaster occurring is low, but the business impact is extremely high.

Major disaster or disruption

- Guidelines for defining this type of event include:
  - This event disrupts all or most of the normal business operations of the company and all or most of its critical business processes.
  - The disruptions occur because all or a majority of systems and equipment have failed or are inaccessible.
  - This includes destruction to the entire facility; a major portion of the facility; or entire networks, subnets, or sections of the business.

Activation Phase

- Once you've defined what this level of disaster or disruption entails, you should define the process for determining which parts of your BC/DR plan should be activated and which team members should be called upon.
- You should attempt to define the business systems, mission-critical functions, and major operations that, when affected, would cause a major disruption.
- This will help you develop appropriate triggers to determine when and how to activate your BC/DR plan.

Activating BC/DR teams

- Clearly, the BC/DR plan cannot activate itself; someone or a team of people need to make appropriate assessments of the situation and make a determination as to whether or not to activate the plan or portions thereof.
- Therefore, it's also important to create and maintain BC/DR teams who handle the response to the business disruption by implementing appropriate sections of the BC/DR plan.

Activating BC/DR teams

- Crisis management team (CMT)
- Damage assessment team
- Notification team
- Emergency response team
- Business continuity coordinator or lead
- Crisis communication team
- Resource and logistics team
- Risk assessment manager

Developing triggers

- Typically, risks and triggers are identified so that if a project risk occurs, a trigger defines when an alternate plan or method should be implemented.
- If you are going to implement your plan, you'll need to define how and when that should occur—those are your triggers.
- For example, if you use the three categories of major, intermediate, and minor, you'll need to define what actions are taken in each case. Each level of disruption should have clearly defined triggers.

Developing triggers

- Let's look at a hypothetical example.
- You're the IT manager of a small firm and the head of the BC/DR team. You're at home one evening just sitting down to dinner when one of the data processing operators who works until 9 PM calls you. She reports that there was a fire in the building, it's been evacuated, and the fire department is on the scene. You ask her a series of questions and ascertain that the fire seems to have been contained relatively quickly but that some of the networking gear may have been damaged either by the fire or by the fire containment efforts. She believes the server room is intact but she's not sure. If you have clearly defined triggers in place, you may determine that this appears to be either a minor or an intermediate disruption and that you should most likely activate a portion of your BC/DR plan.

Developing triggers

- The trigger might be defined as a series of steps such as:
  - Business disruption event has occurred.
  - Disruption to business operations has occurred.
  - Initial assessment by employees on the scene indicates intermediate-level damage, including the following:
    - A portion of the network is or may be out of service.
    - One or more critical servers are or may be out of service.
    - A portion of the physical facility has been impacted by the disruption.
    - It is likely employees will not be able to resume normal operations within 2 hours.

Developing triggers

- This is an example of a trigger you could define for intermediate types of events.
- As you've done previously, using scenarios helps you define these elements more clearly.
- By defining three statements and four attributes, you have a good understanding of whether or not to activate the BC/DR plan for intermediate outages.
- You also have a defined timeline—if normal business operations cannot resume within 2 hours. This should be tied to your overall maximum tolerable downtime (MTD) and other recovery metrics developed earlier. If your MTD is 24 hours, an intermediate disruption might be something that will disrupt normal operations for 2-6 hours. You and your team will need to define these various windows, but be sure to tie your triggers to your recovery metrics.

Developing triggers

- □ Your intermediate activation steps are related to the trigger.
- □ Once you know you should activate your plan, you should define the immediate steps to be taken.
- □ This helps remove any uncertainty about next steps and helps begin a focused response effort.

Developing triggers

- An example of the first steps for an intermediate disruption is shown here.
  - If a disruption appears to be intermediate on initial assessment, within 2 hours:
    - Attempt to gather information from the emergency responders, if appropriate.
    - Activate the damage assessment team.
    - Notify the CMT to be on standby notice.

Developing triggers

- An example of the first steps for an intermediate disruption is shown here (cont.).
  - After 2 hours from event notification, gather initial evaluation from damage assessment team. Analyze data and determine:
    - Take remedial action and resolve issue.
    - Partial or full activation of BC/DR plan.
  - After 3 hours, notify CMT of next steps (stand down, fully activate).
  - Within 3 hours of event notification, BC/DR plan should be implemented if assessment indicates intermediate or major disruption.

Developing triggers

- Notice that the description of the actual disruption levels includes trigger information.
- How many systems are impacted? How extensive is the damage?
- The more clearly you can define these details, the more precise your triggers will be.
- This will help you determine if and when to activate your plan.
- Spend time clearly defining the circumstances that will warrant plan activation at the various levels you've defined.
- Also define initial steps to be taken in each phase so that you have checklists of next steps.

Transition trigger—Activation to recovery

- Another trigger to define is when to move from one phase to another, the transition trigger.
- In this case, that means when to move from the activation phase to the recovery phase.

Transition trigger—Activation to recovery

- Define the transition trigger:
  - The damage assessment team's initial evaluation indicates an intermediate disruption.
  - The CMT has been called in and is on scene.
  - The immediate cause of the event has stopped or been contained.
  - The intermediate BC/DR plan has been activated.

Transition trigger—Activation to recovery

- You may wish to define other triggers for your transition, from activation to recovery, suitable to your organization.
- When defining your triggers throughout, keep your MTD and other defined metrics in mind so that you can work within those constraints.

Transition trigger—Activation to recovery

- For example, if your MTD is very short, your time between activation and recovery also should be very short. In this case, you may have to err on the side of timeliness and take action with incomplete or preliminary data. You'll have to balance your need to collect information with your need to get the business back up and running as quickly as possible (and within your MTD constraints). Rarely, if ever, is there perfect data in an emergency (or any other time). Clearly defining these triggers and constraints in your plan can help you make better decisions in the stressful aftermath of a business disruption or disaster. Help the team make the best decisions possible by spending time now to define these triggers as clearly and unambiguously as possible.

Recovery phase

- The recovery phase is the first phase of work in the immediate aftermath of the disruption or disaster.
- This phase usually assumes that the cause of the disruption has subsided, stopped, or been contained, but not always.

Recovery phase

- For example, in the case of flooding, you may decide that if it's external flooding, you will wait until waters subside to begin recovery efforts. This may be required by local officials who restrict access to flooded areas. However, in other cases, you may be able to or choose to initiate recovery efforts while flooding is still occurring. This might include placing sandbags around the entry ways to the building or removing equipment that is not yet under water. As you can tell, many of your actions will be dictated by the specifics of the situation, so there's no simple rule to follow here. However, we can say that recovery efforts have to do with recovering from the immediate aftermath of the event, whether or not the event is still occurring.

Recovery phase

- This phase may also include
  - evacuating the facility,
  - removing equipment that can be salvaged quickly,
  - assessing the situation or damage, and
  - determining which recovery steps are needed to get operations up and going again.

Transition trigger—Recovery to continuity

- At this juncture, you can make a note that you need to develop triggers that help you know when to transition from recovery efforts to business continuity efforts.
- Typically, these triggers will have to do with determining that the effects of the disruption have been addressed and are not getting any worse.

Transition trigger—Recovery to continuity

- For example, if you experience a fire in the building, the fire is out, the assessment has been done, any equipment or supplies that can be salvaged have been, and alternate computing facilities have been activated.
- Those are activities that take place in the recovery phase and when these are all complete, it's time to move into the business continuity phase, which typically includes starting up systems so that normal business operations can resume.
- Defining these points should include specific events that have occurred, milestones that have been met, or time that has elapsed.
- Also keep your MTD in mind as you define triggers for this transition.

Business continuity phase

- The business continuity phase kicks in after the recovery phase and defines the steps needed to get back to "business as usual."
- For example, if you have a fire in the building, the recovery phase might include salvaging undamaged equipment, ordering two new servers from a hardware vendor, and loading up the applications and backup data on the servers at a temporary location so that you can begin to recover your data and your business operations.

Business continuity phase

- □ The business continuity phase would address how you actually begin to resume operations from that temporary location, which workarounds need to be implemented, what manual methods will be used in this interim period, and so forth.
- □ The final steps in the business continuity phase will address how you move from that temporary location to your repaired facility, how you reintegrate or synchronize your data, and how you transition back to your normal operations.

Business continuity phase

- □ You'll also need to define triggers here that define when you end business continuity activities and when you resume normal operations.
- □ Again, as with the other triggers, you should strive to be as clear and concise as possible.

Business continuity phase

- Certainly, business operations will resume, but some things may change permanently as a consequence of this disruption.
- For example, your company may decide as a result of a major fire or flood that it wants to move to a new location and it's going to do that while operating from the alternate site. That would complicate things because it would mean moving from the alternate site to a new site, with all the related challenges inherent in both resuming normal operations and moving to a new facility.

Business continuity phase

- Another example is developing a work-around that's used in the recovery phase that works so well that someone decides to use it full time.
- When do you transition back to normal operations if you select your BC/DR work-arounds as your new normal?
- When do you officially transition back to normal operations if you decide that the new server role or network configuration actually works better than the original?

Business continuity phase

- It might be a simple matter of formally evaluating the change, agreeing to make it permanent, and declaring you're now running under normal operating conditions.
- However, you now need to back a new BC/DR plan to address a potential failure at your new location—including how and where you store backups generated at this new location.
- You and your team can define these triggers in advance and you may need to modify them later, but at least you won't be starting with a blank slate.

Maintenance/review phase

- □ The maintenance phase has to occur whether or not you ever activate your BC/DR plan.
- □ On a periodic basis, you need to review your BC/DR plan to ensure that it is still current and relevant.
- □ As operations and technology components change, as you add or change facilities or locations, you'll need to make sure that your plan is still up-to-date.

Maintenance/review phase

- One common problem in BC/DR planning is that companies may expend time to develop a plan, but they often do not want to (or will not) expend the time and resources necessary to keep the plan current.
- Old plans are dangerous because they provide a false sense of security and may lead to significant gaps in coverage.

Maintenance/review phase

- □ If a plan is not maintained, then all the time and money invested in creating the plan is wasted as well.
- □ We've repeated it numerous times due to the effectiveness of the approach—seek to operationalize plan maintenance as well.
- □ Ensure that every time you stand up a new server, switch or storage solution that you review how it impacts (and is impacted by) your BC/DR plan.
- □ This review can be an established part of your IT change control process, and your change control documentation can call out any necessary changes to your BC/DR plan as a result of each change.

Maintenance/review phase

- □ In addition, if you end up activating your BC/DR plan at some point, you'll want to assess the effectiveness of the plan afterward, when things settle down.
- □ You should do this relatively close to the end of the recovery and business continuity cycles so that lessons learned can be captured and applied to your BC/DR plan before memories fade and people go back to their daily routines.

Maintenance/review phase

- Reviewing the plan in the immediate aftermath of a disruption will give you valuable insights into what did and did not work.
- Incorporating this knowledge into your plan will help you continue to improve the plan to meet your evolving business needs.

DEFINING BC/DR TEAMS AND KEY PERSONNEL

- □ There are numerous people in positions that are critical to the activation, implementation, and maintenance of your BC/DR plan.
- □ Although these may not all be relevant to your organization, this will serve as a good checkpoint to determine who should be included in your various phases.
- □ You'll also need to form teams to fulfill various needs before, during, and after a business disruption or disaster.

DEFINING BC/DR TEAMS AND KEY PERSONNEL

- A good team description will identify the following attributes:
  - Positions or job functions included on the team (Facilities Manager, HR Director, etc.)
  - Team leader and contact information
  - Team mission statement or set of objectives
  - Scope of responsibilities (define what is and is not part of this team's mission)
  - Delineation of responsibilities in each phase of BC/DR (i.e., when will the team be activated and deactivated?)
  - Escalation path and criteria

Crisis management team

- In most companies, the composition of CMT will mirror the organizational chart.
- It should have representatives from across the organization and should bring together members of the company who have the expertise and authority to deal with the aftereffects of a major business disruption.
- The CMT will decide upon the immediate course of action in most cases and, when necessary, they can contact senior management.

Crisis management team

- They will direct the distribution and use of resources (including personnel) and will monitor the effectiveness of recovery activities.
- They can adjust the course of action, as needed.
- They should be in charge of activating, implementing, managing, and monitoring the business continuity and disaster recovery plan and should delegate tasks as appropriate.

Management team

- Each company has a management team or structure that oversees the business and its operations.
- You’ll need to determine which positions from your management team should be included in your plan.
- Remember to review all the phases.

Management team

- For example, you might decide that only a member of the management team can cause the BC/DR plan to be activated.
- Management might be required to decide when to transition from disaster recovery to business continuity activities or they might be the one(s) to decide how and when the BC/DR plan should be tested.
- In addition, different levels of management may activate parts of the plan or the entire plan, depending on disaster level.
- Identify the positions that should participate as well as define how they should participate in each phase.
- It's important to note that documenting "roles and responsibilities" of disaster responders is a basic legal requirement of most companies which fall under one or more government regulations related to IT security.

Damage assessment team

- A damage assessment team should be comprised of people from several key areas of the company, including Facilities, IT, HR, and Operations.
- Your company's damage assessment team may contain other members, depending on how the company is structured and what type of business you're in.
- If you work in a small software development firm, you may just need the CEO, the IT manager, and the office manager to operate as the damage assessment team.

Damage assessment team

- In larger companies with multiple locations, you'll need to have several damage assessment teams or you may choose to create a mobile team that can fly to any site and assess damage within 24 hours of an incident.
- You may choose to have both a local and a mobile corporate team so that the right team can be called in.
- If the building floods, you may not need the mobile team to come in.
- However, if you have a large fire, earthquake, or other major event, you may need the support services of a mobile damage assessment team.

Operations assessment team

- □ You may choose to have a separate operations assessment team comprised of individuals who can assess the immediate impact on operations.
- □ A damage assessment team may be tasked with this job, but in some types of companies, you may need a separate operations team that can assess what's going on with operations and how to proceed.
- □ The operations assessment team can also be tasked with beginning recovery phase activities, monitoring and triggering the transition from activation to recovery, recovery to business continuity, and BC to normal operations.

IT team

- Clearly, you need an IT team that can not only assess the damage to systems but also begin the disaster recovery and business continuity tasks once the plan is activated.
- This IT team will work closely with the damage assessment team and/or the operations assessment team to determine the nature and extent of damage, especially to IT systems and the IT infrastructure.
- You may not need some of the technical specialties listed here, but this should be a good starter list for you to work from to determine exactly what expertise you'll need on your team.

IT team

- Operating system administration
- Systems software
- Server recovery (client server, Web server, application server, etc.)
- Storage recovery
- Database recovery
- Network operations recovery
- LAN/WAN recovery
- Application and data recovery
- Telecommunications
- Information security team

Administrative support team

- During a business disruption, there are a wide variety of administrative tasks that must be handled.
- Creating an administrative support team that can respond to the unique needs of the situation as well as provide administrative support for the company during the disruptions is important.
- This might include ordering emergency supplies, working with vendors arranging deliveries, tracking shipments, fielding phone calls from the media or investors, organizing paper documents used for stopgap measures, and more.

Transportation and relocation team

- Depending on the specifics of your BC/DR plan and the type of company you work in, you may need to make transportation arrangements for critical business documents, records, or equipment.
- You may need to move equipment in advance of an event (like a hurricane or flood) or you may need to move equipment after the event to prevent further damage or vandalism.
- Relocating the company and its assets before or after a disruption requires a concerted effort by people who understand the company, its relocation needs, and transportation constraints.

Media relations team

- You may need to create a crisis communication plan because you usually will need to provide information about the business disruption/disaster to employees, vendors, the community, the media, and investors.
- One key area that should be well prepped is media relations.
- Unlike other stakeholders mentioned, the media make their living selling interesting stories.
- Since a disruption at your business may qualify as news, you might as well craft the message rather than leaving it to outsiders.

Media relations team

- Creating a team that knows how to handle the media in a positive manner and that understands the policies and procedures related to talking with the media is vital to help ensure your company’s image and reputation are maintained to the greatest extent possible.
- Certainly, if your company is at fault, you will have to deal with a different set of questions than if your company experiences a natural disaster.
- Still, you’ll need to manage the story either way.
- Most mid-sized to large companies have a communications team who handles exactly these kinds of issues, so the team may already be in place.
- If that’s the case, your plan should address how to bring that team into the loop in the event of a disaster.

Human resources team

- The aftermath of a crisis is an incredibly stressful time for all employees.
- Having an HR team in place to begin handling employee issues is crucial to the well-being of the employees and the long-term health of the company.
- Retaining key employees, adequately addressing employee concerns, facilitating insurance and medical coverage, and addressing pay and payroll issues are part of this team’s mission.
- This team may also be responsible for activating parts of the BC/DR team as it relates to hiring contract labor, temporary workers, or staff at alternate locations.

Legal affairs team

- Whether your legal experts are internal or external to your company, you should identify who needs to address legal concerns in the aftermath of a business disruption or emergency.
- If you hire outside counsel to assist you with legal matters, you should still assign an internal resource as the liaison so that legal matters will be properly routed through the company.
- If you operate in a heavily regulated industry such as utility, banking, government, finance, or health care, you should be well aware of the constraints you face, but having a legal affairs team can assist in making decisions that keep your company's operations within the bounds of laws and regulations.

Legal affairs team

- Even if you're not in a heavily regulated industry, you may need advice and assistance in understanding laws and regulations in your recovery efforts.
- These items may be outside the scope of your IT duties, but in small companies where people wear many hats, you may be the only one thinking about these kinds of issues.

Legal affairs team

- □ If you work in a larger company that has legal counsel, you may want to think through any potential legal issues you may face with respect to IT.
- □ For example, if you are a service provider, you may have legally binding service-level obligations that are impacted in a disaster. Having a legal representative step in during a disaster to handle those issues could be helpful.
- □ At minimum, it is prudent to have outside legal counsel review your BC/DR plan for any gaps related to your company's legal obligations to provide "reasonable security" and "security breach notification".

Physical/personnel security team

- In the aftermath of a serious business disruption, you will need a team of people who address the physical safety of people and the building.
- These might be designated Human Resource representatives, security staff, or people from your Facilities group, for example.
- If you work in a large company or in a large facility, you may have a separate security department or function that manages the physical and personnel security for the building.
- If this is the case, designated members of their team should be assigned to be part of the BC/DR team.

Physical/personnel security team

- If you don't have a formal security staff, be sure that the members of this ad hoc team receive training.
- Someone from HR or facilities might be willing to take on the role of security in the aftermath of a disaster, but they need to be trained as to the safest, most effective method of managing the situation.
- Training for part-time or ad hoc security teams is crucial because if a natural disaster strikes, emergency personnel such as your fire or police department will focus on helping schools, day care centers, nursing homes, and hospitals first.
- Your company may fall very low on the list of priorities, so having trained staff that can fill the gap in an emergency may literally mean the difference between life and death.

BC/DR contact information

- After you've developed the requirements for your teams in terms of the specific skills, knowledge, and expertise needed, you'll identify the specific people to fill those roles.
- Part of plan maintenance involves ensuring that the key positions are still in the BC/DR loop and that key personnel are still aware of their BC/DR responsibilities.

BC/DR contact information

- Another mundane but crucial task in your planning work is to compile key contact information.
- Since computer systems often are impacted by various types of business disruptions— from network security breaches to floods and fires— you'll need to have contact information stored and available in electronic and hard copy.
- It should be readily available at alternate locations and copies should be stored in off-site locations that can be accessed if the building is not accessible.

BC/DR contact information

□ However, since this list contains contact information, it should also be treated as confidential or sensitive information and should be handled and secured as such.

□ This information should include contact information for key personnel from the executives of the company (who will need to be notified of a business disruption) to BC/DR team members to key suppliers, contractors, and customers, among others.

BC/DR contact information

- Develop a list of the types of contact information you need, including:
  - Management
  - Key operations staff
  - BC/DR team members
  - Key suppliers, vendors, and contractors (especially those with whom you have BC/DR contracts)
  - Key customers
  - Emergency numbers (fire, police, etc.)
  - Media representatives or PR firm (if appropriate)

DEFINING TASKS AND ASSIGNING RESOURCES

- The tasks and resources that need to be assigned have to do both with implementing the mitigation strategies you've defined as well as fleshing out the rest of the plan.
- First, you have to ensure your risk mitigation strategies will be properly implemented.
- This may mean creating project plans to address any new initiatives you need to undertake in order to meet your risk mitigation requirements.
- We'll assume you've got that covered as part of your risk mitigation strategy.

DEFINING TASKS AND ASSIGNING RESOURCES

- □ If not, now’s the time to develop your WBS, tasks, resources, and timelines for completing any risk mitigation strategies that need to be completed in advance of a disruption.
- □ This might include purchasing and installing new uninterruptible power supplies for key servers, updating your fire suppression systems, or implementing a data vaulting solution.
- □ Other mitigation strategies such as arranging for an alternate site need to be completed in advance, but activating it requires a different set of tasks that occur later.

DEFINING TASKS AND ASSIGNING RESOURCES

- □ Other tasks have to do with defining your BC/DR teams, roles, and responsibilities; defining plan phase transition triggers; and gathering additional data.
- □ Let's start with tasks related to some major activities including alternate sites and contracting for outside BC/DR services. Clearly, there are other tasks and resources you'll need, but this should get you started in developing your own list of tasks, budgets, timelines, dependencies, and constraints for the remaining BC/DR activities in your plan.

DEFINING TASKS AND ASSIGNING RESOURCES

- Processes:
  - Identify high-level tasks and use verb/noun format when possible (i.e., “test security settings” rather than “security settings”).
  - Break large tasks into smaller tasks until the work unit is manageable.
  - Define duration or deadlines.
  - Identify milestones.
  - Assign task owners.
  - Define task resources and other task requirements.
  - Identify functional and technical requirements for task, if any.
  - Define completion criteria for each task.
  - Identify internal and external dependencies.

Alternate site

- If part of your risk mitigation strategy is to develop an alternative site or off-site storage solution, you should develop a number of details before moving forward.
- These should be tasks (or subtasks) within the WBS just discussed, so let's look at some of the details you might include.
- Also keep in mind that you need to develop a trigger that helps you determine if or when you fire up the alternate site. You probably don't want to activate the alternate site if you have a minor or even an intermediate disruption, so how do you define when you should? When all systems are down or when some percentage of systems down?

Alternate site

- □ You have to take your MTD into consideration along with other factors such as the cost of firing up the alternate site and the cost of downtime.
- □ If your downtime is estimated to be 12 days and that cost is $500,000 but the cost of firing up the alternate site is 3 days and $250,000, is it worth it to activate the alternate or should you just hobble along until you can restore systems at the current location?

Alternate site

- There’s no right or wrong answer, it’s going to depend on your company’s MTD, potential revenue losses, cost of starting up the alternate site, and so on.
- Have the financial folks on your BC/DR team prepare some analyses to determine metrics you can use to help determine your trigger point.
- As you’re going through the activities listed in this section, keep these factors in mind.

Selection criteria

- Selection criteria are the factors you develop to help you determine how to select the best alternate site solution for your company.
- This includes cost, technical and functional requirements, timelines, quality, availability, location, and more.
- Be sure to consider connectivity and communications requirements in this section along with your recovery requirements such as MTD.
- Remember that you need to find the best balance between risk and mitigation—so your selection criteria should not be so rigorous as to exclude all but the most expensive, iron-clad options.

Selection criteria

- You may choose to use prioritization in your selection criteria language.
- For example, availability and technical requirements might be your first priority; location might be second or even third.
- By prioritizing, you can ensure you don’t box yourself into a solution that is overengineered (or under-engineered) for your needs.

Contractual terms

- Determine what contractual arrangements are appropriate for your company.
- Many vendors have predetermined service offerings and contracts are fairly standard.
- Other companies can accommodate a wider range of options and will work with you to develop appropriate contractual language.
- In either case, be sure to run these contracts past your financial staff and your legal counsel to make sure you are fully aware of the financial and legal consequences of these contracts in advance of signing them

Contractual terms

- □ If you're not clear what they mean operationally, be sure to talk with the vendor and add clarifying language to the contract.
- □ Do not simply take the vendor's word that a particular paragraph or section means something.
- □ Verbal agreements are always superseded by written contracts, so make sure the contract spells it out clearly.
- □ If the language is vague, confusing, or contradictory, work with the vendor and your contracting or legal department to clarify.
- □ You should never rely on verbal commitments when it comes to implementing your BC/DR solutions, so be sure to put everything in writing in advance.

Comparison process

- Be sure to specify what process you'll use to select the vendor.
- This might include a list of technical requirements the vendor must meet, but it might also include an assessment of the vendor's geographical location, financial history, and stability and industry expertise, among other things.
- Selecting the right vendor for an alternate site or off-site storage is a very important aspect to your BC/DR success and should be undertaken with the same rigor as your other planning activities.
- Again, using prioritization of criteria will help you select the right solution.

Comparison process

- Finally, check references before making a final selection.
- If you can find customers the vendor does not directly supply to you, you’re more likely to get an accurate picture.
- If the vendor supplies you with customer references, be sure to ask that customer some leading questions such as “When you had problems with connectivity, how did the vendor respond?”
- By asking this type of question, you can lead even a reference customer into discussing issues that came up.
- Your intent is not to trick anyone, but to get a clear and accurate picture of the vendor’s capabilities and responsiveness.

Acquisition and testing

- Once you’ve selected your alternate site or off-site storage vendor and completed the contract, you will need to make whatever additional arrangements are needed for developing this solution so that it is fully ready in the timeframe you’ve designated.
- This might include purchasing additional hardware and software, setting up communications channels, and testing all solutions implemented.
- Create a thorough acquisition and testing plan for this phase so you can transition to it as seamlessly as possible in the event of a business disruption.
- During your testing phase of the BC/ DR plan, you should test the process for firing up this solution on a periodic basis.

Cloud services

- Cloud services are one of the newest developments in BC/DR risk mitigation strategies.
- Cloud services encompass many different service offerings, including:
  - IaaS (Infrastructure as a Service)
  - PaaS (Platform as a Service)
  - STaaS (Storage as a Service)
  - DRaaS (Disaster Recovery as a Service)
  - SaaS (Software as a Service)

Cloud services

- Cloud computing allows for the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet).
- Cloud services are typically priced on a pay-per-use basis.
- End users access cloud-based applications through a Web browser or lightweight desktop or mobile application while the business software and user's data are stored on servers at a remote location.

Cloud services

- In the case of SaaS, users are provided access to application software and databases, and cloud providers manage the infrastructure, platforms that run the applications, as well as all IT disaster recovery operations.
- This allows businesses to reallocate IT operations costs away from hardware/software spending and labor expenses associated with IT support, toward meeting other goals.
- Through economies of scale and use of converged, shared infrastructure, cloud providers are typically able to offer similar IT services at a cheaper operational cost.

Cloud services

- In addition, cloud computing allows users to obtain, configure, and deploy cloud services themselves using cloud service catalogs, without requiring IT assistance.
- One major downside often noted with such an arrangement is the increased risk of unauthorized access to sensitive business data should the cloud provider not have consistent security controls in place that meet or exceed business requirements.

Cloud services

- In the most basic cloud service model, providers of IaaS or STaaS offer compute (servers or workstations) and storage as two distinct offerings.
- Cloud providers supply these resources on-demand from their large resource pools in remote data centers.
- For secure connectivity, customers can use either SSL/TLS encryption over the Internet or dedicated virtual private networks (VPNs) with IP-based encryption.
- In the PaaS model, cloud providers offer a full computing platform, which typically includes an operating system, programming language execution environment, database, and/or Web server.
-

Contracts for BC/DR services

- As with alternate site or cloud considerations, keep your MTD, your costs, and potential losses in mind.
- Have your financial folks help you with performing financial analyses to determine what makes financial and business sense for your company.
- If a firm wants to charge you $50,000 for some sort of contract but your downtime estimate with associated revenue and collateral loss is only $40,000, the contract might not be worth entering.
- Additionally, determine your triggers for calling upon these contractual arrangements so you don’t prematurely fire up these contracts or avoid using them during times when they should be activated.

Develop clear functional and technical requirements

- The more specific you are, the more fully a vendor can address your needs.
- If some requirements appear to be optional or "nice to have," then list them as options and not as requirements.
- Pare down your requirements to the elements you absolutely must have.
- Remember, the more options you include, the higher the cost.

Develop clear functional and technical requirements

- Therefore, if cost is an issue (and it almost always is), be sure to list what you require and what you desire as separate items.
- When this information has been finalized, write up formal requirements documents that you can provide to potential vendors.
- Also, be sure that your requirements documents are reviewed by subject matter experts, including IT experts and those in your company who understand regulatory, legal, and compliance issues.
- Your requirements should meet all these needs before going out to the vendors.

Determine required service levels

- Service levels are typically part of technical requirements, but we've listed them separately because they are vitally important when developing Requests for Proposal (RFP) or Requests for Quote (RFQ) from vendors.
- You may have contractual obligations to provide certain levels of service to your customers, so you may need to specify requirements for your vendors that meet or exceed these metrics.
- Even if you have no externally facing service-level agreements (SLAs), you should still specify SLAs in your contracts with vendors.
- If you're contracting for Internet connectivity, you should specify bandwidth, minimum upload and download speeds, and maximum downtime per specified period, for example.

Compare vendor proposal/response to requirements

- Once you receive vendor responses to your proposals, you should evaluate how closely each vendor comes to meeting the requirements of your plan.
- Any vendor that does not meet the requirements should not be considered further.

Compare vendor proposal/response to requirements

- There may be two exceptions to this.
  - First, if your requirements are unique enough that no single vendor can meet your needs, you may have to circle back and find two or more vendors who can work together to meet your unique requirements.
  - Second, you may discover from vendor responses that your requirements were too broad, inclusive, or vague, and that none of the vendors' responses meet your requirements exactly. In that case, you may have to refine your requirements and go back out for bid.

Compare vendor proposal/response to requirements

- Assuming your requirements are well written, your next step is to eliminate vendors that cannot meet your needs and focus only on those vendors who addressed your requirements fully in their responses.

Identify requirements not met by vendor proposal

- If there are one or more requirements not met by any vendor, you may need to find two or more vendors to work together to provide the full range of services you need.
- If none of the vendors met a particular requirement, you may also choose to review that requirement and reassess it in light of vendor responses.
- Remember, you contract with vendors in order to leverage their specific expertise.

Identify requirements not met by vendor proposal

- If none of them meet a particular requirement, you may wish to talk with several of your short-list selections to find out why they did not address that aspect.
- It might be redundant or otherwise unneeded. In that case, you should revise your requirements to reflect this new information.

Identify vendor options not specified in requirements

- Vendors also may offer additional options not specified in your requirements.
- Again, based on the vendor's expertise, they may offer additional choices that can round out your requirements or plan.
- Utilizing their expertise can be a good way of ensuring you have the best solution in place.

Identify vendor options not specified in requirements

- □ For example, the vendor might say (in essence), "Everyone who's asked for A, B, and C also has found that D was an extremely important option they'd overlooked. Perhaps you'd like to add D to your plan as well."
- □ They may be sharing industry expertise and best practices with you or they may simply be trying to up-sell you.
- □ You'll have to look carefully at these options and perhaps do some independent research to determine whether these options are "must have," "nice to have," or "useless add-ons."

COMMUNICATIONS PLANS

- Communications plans can be assigned to other existing teams.
- A good example of this is that the employee communication plan may be the responsibility of the HR team.
- There's no need to create additional teams to execute communications plans if these activities fall within the scope of defined teams.

COMMUNICATIONS PLANS

- However, in some companies, it might make sense to have most of the communications come from one dedicated communications team in order to maintain control over communications and to ensure that a single consistent message is delivered to all stakeholders.
- The decision is yours and usually is based on how large the company is and how it currently operates.

Internal

- The internal communication plan is really part of the BC/DR activation and implementation plan.
- If a business disruption occurs, you need to have a process in place for notifying BC/DR team members.
- This is done as part of BC/DR plan activation and is a critical aspect that should be clearly delineated.
- How will team members be notified and updated? What processes, tools, and technology are needed? Are these included in your plan yet? If not, add them to your project plan's WBS or in a section called Additional Resources so they are captured and addressed in advance of a business disruption.

Employee

- Employee communication is also internal communication but differs because it is any communication that goes out to employees who are not part of the BC/DR activation and response team.
- If a business disruption occurs, you'll need to know how to notify all employees.
- You'll also need to let them know answers to the most basic questions including what happened, what is being done to address the problem, and who they should go to for more information.

Customers and vendors

- Customers and vendors typically require different types of communications but the information is often similar.
- They may need to be notified of the business disruption, the basic steps being taken to rectify the problem, the estimated time to recovery, and any work-arounds needed in the meantime.
- Knowing how to communicate in a disaster is a skill that can be taught and someone in your company should be responsible for that.

Shareholders

- If you have shareholders of any kind (debt or equity investors, shareholders, etc.), you must communicate the nature and extent of the disruption.
- In most cases, they are concerned with the ongoing viability of the company and possibly the short-term financial impact of the disruption on the company as well as any legal liability.

Shareholders

- Therefore, communication with this group requires that specific issues be addressed.
- As you can tell, these issues are very different than, say, employee issues, so someone well versed in investor relations should be charged with this communication.
- In most companies, this task falls to the CEO or a high-ranking corporate officer who can specifically address the concerns of those who have a financial stake in the company.

The community and the public

- □ In addition to communicating with all the other stakeholders we've mentioned, you also will need to communicate with the general public.
- □ Local newspapers, TV, and radio stations will certainly take an interest in a localized business disaster such as a fire or flood.
- □ National and international media may also take interest if the event is unique in some way or is part of a widespread disaster.

The community and the public

- Members of the local community may also have more than just vicarious interest—they may need to understand the impact your business disruption may have on them.
- Businesses in communities don’t exist in isolation, and what happens to one business may have a ripple effect on other businesses even if those other businesses are not customers or suppliers.

EVENT LOGS, CHANGE CONTROL, AND APPENDICES

- □ Event logs, like emergency communication, can become the basis of legal action, so be sure to understand the requirements and constraints various kinds of emergency reporting may have on your company.
- □ Event logs help you keep track of what's going on, what's been done, and what needs to be done next. Keeping detailed logs in real time helps keep track of details that might later be lost.

EVENT LOGS, CHANGE CONTROL, AND APPENDICES

- □ Your company may be required to meet certain legal or regulatory reporting requirements.
- □ Event logs can be helpful in ensuring you meet those requirements.
- □ Consult with legal counsel if necessary and include these requirements in soft or hard copies of your logs.

EVENT LOGS, CHANGE CONTROL, AND APPENDICES

- Changes to the BC/DR plan should be tracked and noted so that team members can easily determine if they have the latest revision of the document as well as the general nature of those revisions.
- Be sure to develop a distribution system that notifies team members of new revisions, provides a method for accessing new documents, and reminds teams to print and store the documents in locations accessible both on- and off-site.

EVENT LOGS, CHANGE CONTROL, AND APPENDICES

- BC/DR plans should be treated as confidential documents.
- They should be handled and stored in a secure manner and old copies should be destroyed appropriately.

EVENT LOGS, CHANGE CONTROL, AND APPENDICES

- □ Information that should not be included in the body of the plan but that is nonetheless vital to the plan should be included at the end as an appendix.
- □ Appendix data can include event log or other document templates, vendor contracts, technical specifications, SLAs, customer contacts, or any other relevant data that would be useful to have along with the BC/DR plan if/when it’s activated.

Reference

- Snedaker, S., 2013, Business Continuity and Disaster Recovery Planning for IT Professionals, Chapter 7.