

College of Business

# Business Continuity and Disaster Recovery (BCDR)

Business Continuity Plans (BCP) &  
Disaster Recovery Plans (DRP)




Image Source: [Pulsant](#)

IT Auditing

Oregon State  
UNIVERSITY

IT risk management guidance and IT audit norms have always emphasized appropriate planning for a disaster, but natural and other disasters have been largely and correctly considered low-probability events. As a result, controls for these risks have been frequently neglected in years past.

More recently, preparing for the worst has become more in fashion. And, applying risk assessment tools this makes sense.

When the only perceived threat that would crash entire systems was a natural disaster or war, most audited organizations would sensibly use a low likelihood in quantifying disaster risk. Even if the cost of rebuilding IT would be crippling, when the chance is very low, - far far less than 1% per year – exposure is also low making it hard to justify costly investments in protections that will never be needed. As a result, except in a few organizations – perhaps government, military, and finance – IT investments to improve operational capability made a lot more sense than investment in Business Continuity Disaster Recovery (BCDR) capability.

But that has changed in recent years. Perceived threats seem more likely as risk managers contemplate climate related factors such as floods or storms, cyber issues including ransomware, and increased threatening political/social events.

While this change of perspective may be speculative, it is a mathematical reality that, together, those possibilities pose a larger threat as compared to just the chance of an earthquake, flood, or fire.

Further, the rise of cloud services had radically changed – reduced – the cost of protecting against catastrophic failure.

In any case, there are many things organizations can, and probably should, do to cost effectively reduce residual risk through BCDR planning.

# Contingency Planning and FISCAM

- The CP – contingency planning component of the FISCAM framework includes two components”
- Management designs and implements controls
  - Achieve continuity of operations [...] in the event of disruption, compromise, or failure
  - Prevent [...] disruption and damage [...] due to natural disasters, structural failures, hostile attacks, or errors
- A few highlights from Table 13:
  - Continuity: Prioritize, plan, people, test
  - Recovery: Risk selection, alternate sites and security mechanisms, maintenance

Table 6: *Critical Elements and Control Objectives for Contingency Planning in FISCAM* lists two critical elements.

Table 13 in FISCAM is dedicated to control activities, audit procedures, and relevant sources of criteria for contingency planning.

CP.01 Management designs and implements control activities to achieve continuity of operations and prioritize the recovery and reconstitution of information systems that support critical or essential mission and business functions in the event of a system disruption, compromise, or failure.

- CP.01.01 Criticality analyses are performed to prioritize mission and business functions and determine the criticality of information systems, information system components, and information system services.
- CP.01.02 Information system contingency plans and other organizational plans are established and implemented to continue critical or essential mission and business functions in the event of a system disruption, compromise, or failure, and to eventually restore the information system following a system disruption.
- CP.01.03 Information system users and other personnel are trained to fulfill their roles and responsibilities associated with the information system contingency plan in the event of a system disruption.
- CP.01.04 Information system contingency plans are periodically tested to determine their effectiveness and the entity’s readiness to execute them.


CP.02 Management designs and implements control activities to prevent or minimize system disruption and potential damage to facilities, information systems, and information system resources due to natural disasters, structural failures, hostile attacks, or errors.

- CP.02.01 Environmental controls are appropriately selected and employed based on risk.
- CP.02.02 Management has established alternate sites, services, and information security mechanisms to permit the timely resumption of operations supporting critical or essential mission and business functions in the event of a system disruption.
- CP.02.03 System backups are regularly conducted and system media containing backup data and software are properly maintained to facilitate the recovery and reconstitution of information systems following a system disruption.
- CP.02.04 Maintenance of information system components is properly performed on a timely basis to prevent or minimize system disruption.

College of Business

## BCP vs. DRP

- BCP and DRP have similar goals, but different orientations.
- Both require the commitment of senior management.
- Business Continuity Planning (BCP)
  - Focuses on continuing to offer key **business services** during disasters.
- Disaster Recovery Planning (DRP)
  - Defines technical requirements for **recovering IT infrastructure**
- Both need “rigorous planning and commitment of resources.”



3

Notably, both BCP and DRP refer to processes – not just plans.

BC focuses primarily on business processes which can be executed to support key activities during a disaster.  
DR focuses on getting computerized systems up and running.

Without the support of senior management, departments will struggle to prepare and coordinate so as to be able to effectively deal with disasters.

## BC and DR

- Key ideas in Business Continuity
  - prioritize mission and business functions and determine the criticality
  - plans are established and implemented
  - system disruption, compromise, or failure
  - personnel are trained to fulfill their roles and responsibilities
  - plans are periodically tested
- Key ideas in Disaster Recovery
  - controls are appropriately selected and employed based on risk
  - established alternate sites, services, and information security mechanisms
  - System backups are regularly conducted and system media containing backup data and software are properly maintained

See 4.4.4 Business Continuity and Disaster Recovery Controls in the ISACA IT Audit Fundamentals study guide, pp 146-148



4

NIST SP 800-34r1 – Contingency Planning Guide for Federal Information Systems defines as disruption this way: An unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

There is a lot to think about. Auditors need to understand these elements if they are to afford reasonable assurance that the BCDR plan has a good chance of being effective when it is needed.

- Prioritization is vital. Organizations need some systems back online quickly to reduce the negative impact of a disaster. They want to focus resources on the most important things first. It would be easy to squander resources on lower priority systems or processes if you don't carefully prioritize in advance.
- Acceptable BCDR plans are not just ideas. They are concrete and include documentation to help during the crisis. And they are supported by real investments in organizational capabilities.
- Leaders need to understand when to "trigger" various components of the BCDR plan. When a crisis arises, information about conditions may not be readily available. If people hesitate to notify the right people or to take action, damage may be multiplied. On the other hand, costly measures should not be taken too quickly or without appropriate approval. Indicators that quantify or characterize an event, whether that be a disruption, compromise, or failure, need to be thought out in advance so that all the team members can operate from the same, thought-out playbook.
- People need to acquire needed knowledge and skill in advance. People don't often rebuild the systems they use, they may not know how. Further, without a clear plan it may not be clear who should do what in a time of crisis. As the old saying goes, proper prior preparation prevents poor performance.
- A plan that has not been tested won't work when it is needed. Modern IT systems are immensely complex. If you haven't walked through recovering the systems, you probably don't have access to something you need.
- Risk quantification: likelihood/frequency \* impact = exposure, residual risk, and the cost of controls should be considered in prioritizing continuity and recovery plan elements.
- A key issue is where. Depending on the disaster, more than one building, location, or city may be affected. That's even true if your systems reside "in the cloud" on a cloud vendor's systems.
- Infrastructure and security mechanisms need to be well understood. If you can't get to the control panel (logically through a network or physically at a location) you can't work on recovery. There is a lot to be said about what resources need to be available offsite, auditors will want to make sure plans account for logistics.
- Backups are THE key element in a recover plan. The right data has to be backed up and the backup copies have to be stored in a location and manner that allows access in a crisis. First, they have to be "off site" so that the disaster that knocks out the systems doesn't render the backup unavailable. But that's only one element. Do you have what you need to restore?

College of Business

## Causes of Disasters

- Disasters that trigger a response plan can arise from various causes
  - Purposeful human attacks
  - Non-malicious Human actions
  - Natural calamities
  - Creeping problems (infrastructure)
    - Starts as a minor issue, but gradually escalates.

Oregon State  
UNIVERSITY

5

Cybersecurity processes often focus on particular systems or particular data in light of known threats.

But we also are concerned with cataclysmic events where entire systems are wiped out. It is all a matter of degree and there is no clear distinction between a moderate loss and a disaster. Solid cybersecurity watches out for catastrophes as well as annoyances.

Four causes of disasters are identified:


1. Cybersecurity often focuses on human threat agents who mean to harm an organization.
2. Mistakes or neglect by individuals within an organization pose meaningful threats addressed by systematic cybersecurity processes. Human problems include accidental file deletions, untested software releases, intrusions, and viruses. Incidents such as these can have massive consequences in some cases.
3. Earthquakes, fires, floods, acts of terrorism, and wars can devastate systems and infrastructure.
4. And, insidiously, relatively small problems, when neglected, can fester and cause cascading or very harmful failures.

A good BCDR process will intentionally account for incidents that arise from any of these causes.

College of Business

## Business Impact Analysis (BIA)

- Evaluate organization processes:
  - The resources/infrastructure needed to run each key process
  - Vulnerabilities and threats to the organization
  - Probability and impact of each threat
- Provides the basis for the Business Continuity Plan (BCP)
  - Prioritize health and safety
  - Help the organization survive the crisis
  - Try to reduce the negative consequences



6

Business Impact Analysis (BIA) is a key step in establishing a business continuity plan.

Prioritization in the BCDR plan will be driven by BIA.

Appropriate managers need to review and approve of the analysis. The board of directors is responsible for BIA at a high level.

Not all systems are equally important.

Some systems need to be up or else replacement functionality has to be provided so that people remain safe. Responsible BCDR's always prioritize health and safety issues.

Then, financial, operational, and reputational impacts need to be considered.


Some examples:

- At a university, a plan may be needed to make sure students in the dorms have access to dining facilities within 12 hours. If the payment systems are computerized and down, decisions need to be made.
- A bank can't afford to forget a bunch of transactions that have already happened.
- Amazon and other large online retailers might lose millions for every hour they are down. Understanding the impact will drive restoration and resiliency investments.

## BIA and BCP Metrics

College of Business

- **RTO: Recovery Time Objectives**
  - How long can the system be down before our reputation, compliance, or operations are threatened?
- **RPO: Recovery Point Objectives**
  - How many minutes/hours/days of data can we lose?
- **MTO: Maximum Tolerable Outages**
  - How long can the firm operate in disaster mode?
- **SDO: Service Delivery Objectives**
  - Which parts of the processes have to work after a disaster? How well do they have to work?



7

Here are some metrics often used in planning efforts. These sound similar but they all impact decisions a bit differently.

Example RTO: “We need to be able to get the order entry system back up within 72 hours.”

Example RPO: “We cannot lose more than 60 seconds of transaction data.”

Example MTO: “We can only run the alternate system/process for one week.” (MTO is very similar to RTO, but focuses on the internal viability of operating in disaster mode.)

Example SDO: “We must continue to offer at least partial billing services during a disaster.”

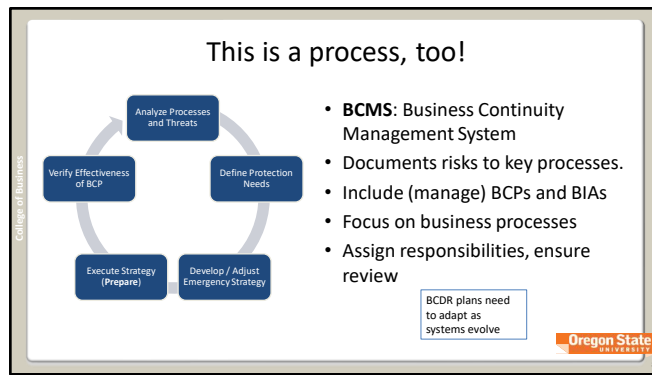
Every system is important. Organizations don’t generally build or operate systems they don’t need.

But in a crisis, priorities matter a lot. Specific, quantified time targets and other clear service objectives help an organization make the difficult choices about what to plan to do first.

Do you see how these might guide planning and investment?

- If a system has a relatively long RTO (say a week) the organization may be able to avoid investing in a “hot site”. It might be enough to have a contract with a computer supplier to deliver new equipment in 48 hours rather than having a redundant system completely ready to go at an alternate location. This could also impact the complexity and cost of ongoing BCP testing. Given a bit of time, many problems are much easier to solve.
- If a system has a long RPO (say 48 hours) that might mean that backups can be run less often. Perhaps the related files need only be included in daily backups. For those data, costs can be reduced by not implementing offsite real-time replication. For example, avoiding the risk of losing changes to the layout and images on a web site might not justify a large investment. The developers could probably reproduce any changes from the last few days from other sources. It would be a hassle, but if a big cost is saved, a little potential hassle in the case of a crisis may be worth it.
- If a longer MTO (say two weeks for a web site or donation portal) was specified. An organization such as a University, or a small non-profit could decide that the money spent on system infrastructure was better deployed in meeting mission through scholarships or service. It would be bad, but we can survive in the unlikely event of a catastrophe.
- All such decisions depend on SDO. There is rarely a single MTO, RPO, and RTO that applies across all of an organization’s systems. Even a small organization is likely to have systems that need to work correctly and quickly and others that could be offline for a good while before organizational objectives are severely compromised. Determining these priorities is, perhaps, the most important part of a business impact analysis process.

Decisions like this are multifaceted. Sometimes its easier, cheaper, and safer to protect all your data “the same way” avoiding the chance that something is mischaracterized or that having different processes can result in something getting missed. Still, quantifying and/or specifying risks using this kind of metric is an important part of assuring an organization can survive a disaster.



BCMS is a process. ISO has standards for such systems. Organizations can compare their processes to standards such as ISO 22301 / ISO 27031.

BCMS may involve the use of software or automated systems, but the big idea is to have a well-defined and systematic process for preparing for inevitable IT incidents. Do you see the difference? A BCMS might well refer to system backups or store risk analyses and a BCP but the BCMS itself is about managing the process of managing disaster risks. That management is done on an ongoing basis by planning, monitoring resources, etc.... It is not a system that is only used in a disaster, and it is not focused on routine tasks such as doing backups.

Implicit in this process is an understanding that as systems evolve, business continuity plans and recovery plans need to adapt. Organizations also continually learn more about threats.

In short, organizations can't make a plan and stick too it for a few years. If the BCDR process does not include continuous improvement, it is deficient.



# Disaster Recovery Testing

- FISCAM: *CP.01.04 Information system contingency plans are periodically tested to determine their effectiveness and the entity's readiness to execute them.*
- From ISACA: Disaster Recovery Testing Steps
  - Develop test objectives
  - Execute the test
  - Evaluate the test
  - Develop recommendations to improve the effectiveness of testing processes and recovery plans
  - Establish a follow-up process to ensure that the recommendations are implemented

ISACA IT Audit Fundamentals study guide, p 148



9

Auditors will usually work with clients to establish credible sources of criteria.

Often any one of several should be fine for the auditor – so long as a minimum level of credibility and coverage is judged to be in place.

The ISACA guide lists some concrete things and IT auditor can look for to evaluate the plan testing process.

Think about the questions the auditors might ask or the other audit procedures they might perform based on this list.

- What are the test objectives? That is, what is supposed to be learned or verified from the testing? Time to restore? Quality of the restored services? Currency of restored data? Performance of the restored system?
- When was/is testing done? How frequently? What documentation is generated?
- How do you evaluate the test results? What do you look for?
- What recommendations or conclusions came out of the test? Did you learn to restore things better next time? Or did you learn ways to improve the effectiveness of future tests?
- How do you follow up to see that lessons learned lead to improvements?

As is so often the case, the auditor is more concerned with an ongoing process that can lead to improvement over proof that a particular test was successful. Of course, if none of the testing is successful, that is an indication of the effectiveness of planning efforts.

## Hot Sites, Backups, and Transportation

- Disasters impact communications
- Responders need to know where to be and need to know how needed resources will be delivered
- Plan to obtain needed equipment
- Reliable and available backups are required:
  - Are they designed and tested so that appropriate RPO and RTO can be achieved?
  - Are copies of needed data, configurations, and programming stored where they will not be lost in a disaster?
  - Are backups protected from unauthorized access or alteration?
  - Failover and backup are different
  - Are multiple version kept to protect against corruption?
  - Are backups protected from errors when files are open?

A key part of a BCDR identifies responsibilities and provides contact information. Mobile phone numbers or, for higher value plans, radios or satellite connections have to be available for communicating with responders, decision makers, authorities, and partners. Some organizations store or keep vehicles and other equipment available at remote locations for emergencies.

Consider this simple but compelling observation. Oregon State University and the City of Portland are in the same subduction zone. In the case of a major earthquake, if buildings or telecommunications in Corvallis are damaged, Portland may be down too. Oregon State University's plan for restoration of services in the case of an earthquake should not depend on Portland-based facilities.

If systems need to be brought up quickly, hot sites are constantly maintained with equipment, programs, and data able to take over. Or a cold site may be identified. Planning ranges from very hot to very cold.

- A hot site's computers and other equipment may be loaded and ready for failover (very hot – very expensive)
- Contracts may be in place so that a vendor will ship replacement equipment on a "next flight out" basis. (less hot/expensive)
- Current manuals and documentation need to be stored in a way that allows access despite major system failures and available to the people who are going to respond to the crisis.

Backup systems need to be set up to achieve appropriate RPO and RTO.

Banks are likely to pay set up (and pay big money for) failover systems that ensure transactions are simultaneously recorded in database versions at multiple locations. It just won't do to "forget" that a million dollars was transferred just before an earthquake. RPO is effectively zero. No data is lost in the case of a failure.

Most other organizations can afford to lose a few minutes, a few hours, or a day's worth of transaction data. Systems that backup and transfer the data to a remote location on some determined schedule will work in that case. Restoration times are also impacted by backup storage choices. Backups may be copied to tapes or to media that can't be accessed quickly. Restoring a lot of data could take many hours. These options are all workable depending on the organization's needs. But the organization needs to have a plan.

Backups that keep track of data as of last year, last week or two days ago can be important. Ransomware or other kinds of data corruption can damage recent backups. Having a failover system is not the same thing as having systematic backups. Also, backups take time and may not be usable if taken while data files are in use. Powerful database management systems can help with this issue, but backups need to be carefully setup and monitored or else, as frequently happens, data are not available when needed.

Auditors need to be sure that the organization reflects such considerations in its BCDR planning.

## Types of Backups

- **Full:** completely copies every file on the file system
  - Slow upfront – can you finish in the available time window?
  - Requires more total backup media space
  - Unique/complete repository = simplified and reliable RTO
- **Incremental:** copies all files changed since the last backup
  - Shorter backup windows, less space, longer restoration times
  - Cheaper to do more frequently, supports strict RPOs
- **Differential:** copies all files changed since the last full backup
  - Characteristics somewhere between Full and Incremental

Certification exams often ask test takers to differentiate between categories so as to demonstrate understanding. Consider:

- It always takes time to copy data. Systems that support faster copying are more expensive.
- It is tricky to back up files that are currently in use.
  - Database management systems have special tools (such as snapshots and logs) to support continuous operation, but special procedures are required to ensure recovery is possible.
  - Many organization 'run' around the clock (e.g., have employees around the world) and users often leave files open even when they are not using them. You have to deal with locked files one way or another.
  - Often organizations have 'backup windows' in that most all their data resources are not in use for a few hours in the middle of the night (a backup window). But if it takes 8 hours to copy the files a two hour window may not be enough.
- You often want to restore only a few files. How hard is it to find the latest version of a file if backups are spread across multiple tapes or stored in multiple repositories? Systems to track multiple versions of a particular file can be complex and expensive.
- If multiple repositories may contain different copies of a file, you may have to read through multiple lists of backed up files.
- Storage space and keeping track of various backup sets costs money. Smaller backup files and shorter file listings (indexes) can result in costs savings.
- The ISACA IT Audit Fundamentals study guide (p145) differentiates these three backup types.

Consider, for example, an old document that rarely changes. Full backups will copy this file over and over again. That uses up space and adds to the length of the indexes. That file would not appear in incremental or differential backups because it hasn't changed. On the other hand, a file that changes daily will be included in each and every backup – no matter the type.

A Full backup has everything. That makes the files larger as compared with the others. But it also means all the files are listed in a single index. To restore a file from a full backup you only have to look at one index containing all the files – that makes restoration fast. Incremental backups are the hardest to search – you have to check every list (starting with the newest one) until you find a copy of the file. But the files and lists are smaller. With differential backups you only have to consider two lists at most: The latest differential and the full. Since, in most organizations, most files rarely change, differential backups tend to be much smaller than full backups.

While those descriptions are true – you can generally find and restore a file from a full backup more quickly than you could if the backups were incremental or differential – sometimes organizations use integrated backup systems that can manage multiple backup sets. In that case it may not take longer to find the latest backup of a particular item, even in an incremental or differential backup. The idea: consider how to back up so that you can restore in an acceptable time frame always applies.

# Auditing Business Continuity Controls

- Understand business continuity needs for this organization
- Inspect/review BIAs, check that RPO and RTO are addressed
- Inspect test results and related process expectations
- Evaluate the availability of needed/useful backups
- Evaluate the ability of personnel to respond as needed
- Ensure that the process for maintaining plans is effective
- Ensure plans are written so that the users will understand

ISACA IT Audit Fundamentals study guide, p 147



12

The ISACA study guide lists things an auditor should do as the assess business continuity efforts.

## Paraphrasing:

- Understand how it aligns with the organization. This is almost always the first step in auditing any control.
- If the process is good, the organization conducts and builds on Business Impact Analysis. The auditor should be able to see evidence of this.
- Check on the currency of the plan; ensure that objectives such as RTO and RPO are appropriately addressed in the planning process.
- As discussed in earlier slides, make sure the tests demonstrate effectiveness.
- There are a lot of ways backups can go wrong. Do the organization's backup processes meet expectations?
- Are personnel prepared to respond?
- Are the plans systematically and effectively managed, and updated for both scheduled and unscheduled changes?
- Are the manuals and plans understandable for the people who will use them?

These are all concrete lines of investigation where an auditor can compare the organization's BCDR planning and capabilities to validate reasonable assurance of effective response to a disaster situation.

The instructor comments that ISACA says that auditors "ensure." Be careful not to infer that the auditor does anything direct to create, develop, or adapt a control process such as BCDR planning. They do the "determine whether" part not the "make it so" part. Their input may guide changes and their findings may spur responses, but it is management that is obliged to manage controls for risk. ISACA's use of the term "ensure" makes the built point concise, but leaves room for mis-interpretation.

This matters because sometimes practitioners think it is up to the auditor, for example, to review the plan for weaknesses when the auditor is actually charged to make sure management as reviewed the plan for weaknesses. When managers leave such tasks to the auditors it means they are thinking of risk management as a "check the box" activity. They may get away with that, but it is not how things are "supposed to be."

The instructor can recall a security manager who said that reviewing lists of accounts with privileged access was an audit task. And perhaps they meant that some IT pro ought t be assigned to audit things once in a while. But that is quite different from the role of an auditor as envisioned by ISACA.