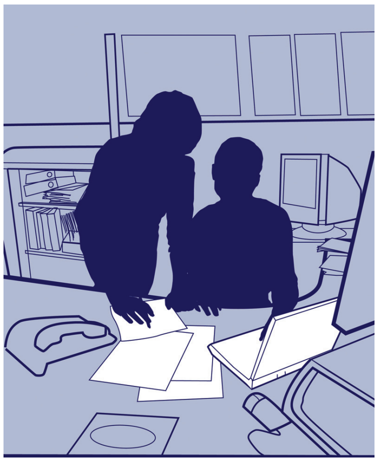
Disaster Recovery and Business Continuity

Barbara Nollau



RUPERT KING/GETTY IMAGES

"Computer Systems Quality and Compliance" discusses practical aspects of computer systems and provides useful information to compliance professionals. We intend this column to be a relevant resource for daily work applications.

Reader comments, questions, and suggestions are needed to help us fulfill our objective for this column. Suggestions for future discussion topics or questions to be addressed are requested. Case studies illustrating computer systems quality and compliance issues by readers are also most welcome. Please send your comments and suggestions to column coordinator Barbara Nollau at barbara.nollau@av.abbott.com or coordinating editor Susan Haigney at shaigney@advanstar.com.

KEY POINTS

The following key points are discussed in this article:

- In today's environment of technology and automation, it is important to understand disaster recovery (DR), business continuity (BC), and contingency plans (CP) and how they all work together to ensure continuity and integrity of systems and availability of data and records
- System owners and technology professionals should understand how these plans should be developed and when/how to exercise them
- Having a DR plan in place is important to the compliance of computer system validation and Part 11 for regulated systems
- The DR team and the associated roles and responsibilities should be clearly defined and understood
- Disaster identification, notification and coordination processes, communication plans, alternate computing facilities management, return to normal operations, plan testing, and maintenance procedures are all required elements of a robust DR program
- Minimally, a company should have a functional plan that addresses all of the processes required to restore technology, an individual responsible for that plan, and a disaster response team at the ready.

INTRODUCTION

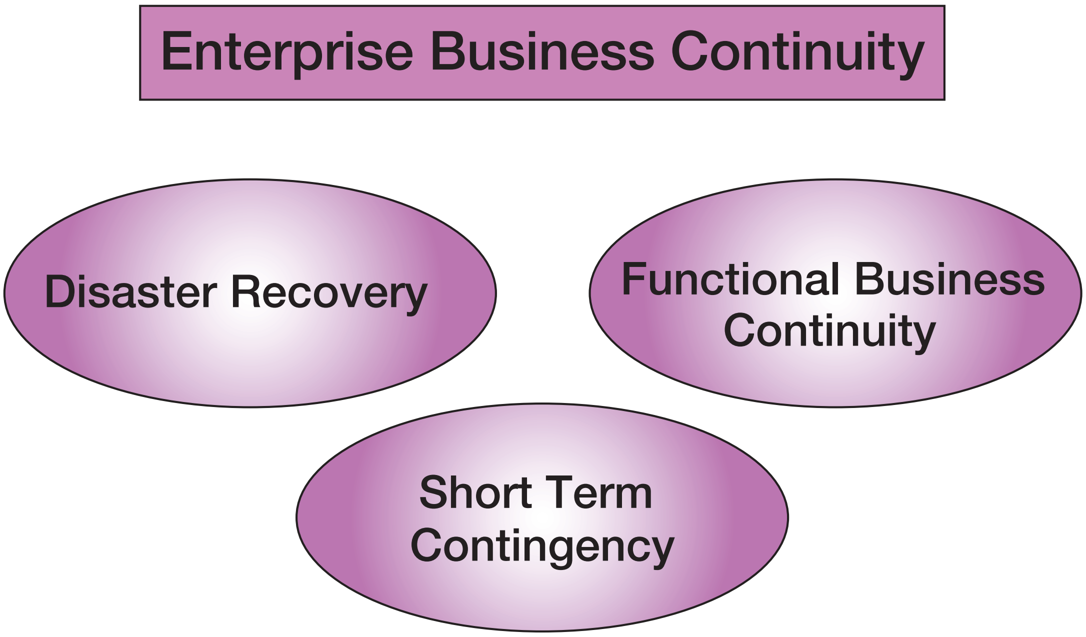
I attended a disaster recovery conference a while back, and one of the speakers said, "If you want to see how real experts plan disaster recovery, go to Puerto Rico–why? Look at the number of hurricanes they deal with on an annual basis. They'd better know what they are doing from a disaster recovery standpoint!" I never forgot that statement, and I've been interested in best practice relative to disaster recovery ever since.

In this issue of the column, we will examine the terms "disaster recovery," "business continuity," and "contingency planning." Understanding these terms and implementing these measures are important for the integrity and compliance of the systems we use. We will further explore the disaster recovery (DR) element to gain a deeper understanding of what is required.

THE MEANING OF "DISASTER"

Webster's defines the word "disaster" as "great distress, destruction, or

Figure 1:
Elements and hierarchy of a DR/BC/CP program.


Enterprise Business Continuity
Disaster Recovery
Functional Business Continuity
Short Term Contingency

misfortune." A disaster is an event that is catastrophic to the business, meaning people can't work, or even worse. An example of a disaster in this context is an earthquake that destroys an entire facility. A smaller event may also be considered a disaster in some cases, for example a fire in a data center that brings all computing capability in the company down. A disaster can be defined as any unplanned event that prevents an entire organization from functioning as intended or causes damage to people or facilities (e.g., fire, explosion, or extensive building damage).

A disaster can have a significant, direct impact to a firm's ability to continue business processing. There may be an inability to develop submissions or collect clinical trial data, delayed or limited ability to get information to the field or process sales data, or the inability to manufacture, pack, ship, or track product, samples, and promotional material. The ability to sustain time sensitive processes such as payroll may also be hindered, effecting financial relationships. The enterprise may be unable to communicate internally or with customers, and there could be residual outcomes such as non-compliance with regulations and lack of alignment with a parent company and partners. Some of the effects of these outcomes are financial in nature (lost revenue from inability to ship product, loss of sales from delayed submissions, loss of worker productivity, or damaged credit rating from inability to pay bills). The company's reputation with customers, employees, partners, or other stakeholders may be damaged.

There is a difference between a disaster and an outage or fault, which is the temporary loss of some or all services (e.g., hard drive failure, power outage, loss of network connection). Localized system outages and brief periods of system downtime (i.e., a document control system down for a day or e-mail unavailable for several hours) are not considered disasters and are, therefore, treated differently, usually with simple contingency plans. What constitutes a true disaster for a company should be defined up front, including determining criteria. This must be understood ahead of time, so it is clear what conditions will lead to invocation of the DR plan. Depending on the magnitude of a disaster, invocation of the broader business continuity (BC) plan may or may not be warranted (DR and one or several functional area BCs may suffice.) Disaster recovery is designed to recover from a true disaster, not an outage or fault.

ELEMENTS OF THE DR/BC/CP PROGRAM

Now that we have reviewed what constitutes a disaster and how that differs from an outage, we need to gain an understanding of the elements of a DR/BC/contingency plan (CP) program, how they work together, and for what conditions each element is used. The elements and hierarchy of the program are shown as follows (see Figure 1):

- **Enterprise business continuity (EBC).** A broad program that covers all aspects of the business (e.g., process, technical, physical, human, etc.). Focuses on keeping the business viable in the event of a disaster.
- **Disaster recovery (DR).** A program focused on technology recovery in the event of a disaster, an element of EBC.
- **Functional business continuity (BC) plan.** A functional area- or business area-specific plan

focused on keeping business processes moving in the event of a disaster, an element of EBC.

- **Contingency plans (CP) for system downtime.** A functional area- or business area-specific process used as a workaround during non-disaster system outages, usually contained in an operating procedure.

The broadest level of BC (enterprise level) covers facilities, human resources, safety, equipment and furniture, communications (internal and external), and invocation of lower level plans. Disaster recovery is focused on technology only and covers the recovery facility (on-site, hot site, or cold site), computer hardware, operating systems, networking, and other infrastructure, application software, databases, and records. Functional BC plans are lower level plans specific to a functional area or given business process. They are usually put in place for critical business processes and cover the manual workarounds to be used until technology is recovered. These workarounds may involve the use of log books, cell phones, hard copy documents, etc. in place of the technology that is unavailable. Finally, contingency plans for system downtime are similar to functional area business continuity; however, they cover localized outages only (e.g., one department, one system, etc.) They are usually feasible for short durations only, assume some sort of infrastructure being in place, and typically involve paper-based manual workarounds.

Developing and maintaining a tested DR/BC program is important to the computer validation process and to compliance with *21 CFR Part 11*, *Electronic Records and Signatures.* A commonly accepted definition for validation is "establishing documented evidence which provides a high degree of assurance that a specific process [system] will *consistently* produce a product meeting its predetermined specifications and quality attributes." In order to address the "consistently" portion of the definition, as part of system validation the following should be verified as in place and tested:

- Disaster recovery plan
- Backup plan
- Business continuity plan
- Contingency plan for system downtime.

Maintaining Compliance

Another validation-related consideration is regarding the maintenance of the validated state of regulated systems/infrastructure. In the case of a major disruption to service that requires restoration in a completely different environment and/or replacement of major components, measures must be taken to ensure the validated state of the system is maintained. A disaster, and subsequent DR, interrupts the qualified state of the IT infrastructure. Once the environment is restored, some level of re-qualification must be performed. The level of re-qualification should be based on risk (risk level of the affected system(s), level of change, and planned sustainability of change). The re-qualification criteria should be pre-determined and documented in the DR plan.

Requirements listed in *21 CFR Part 11* (1) that are related to, amongst other controls, DR are the ability to generate accurate and complete copies for review and inspection, and that records must be retrievable throughout required retention time. In the case of a disaster, without a DR plan, we cannot say that we are able to produce accurate and complete copies or that the records will be retrievable during that time.

DISASTER RECOVERY PLANS

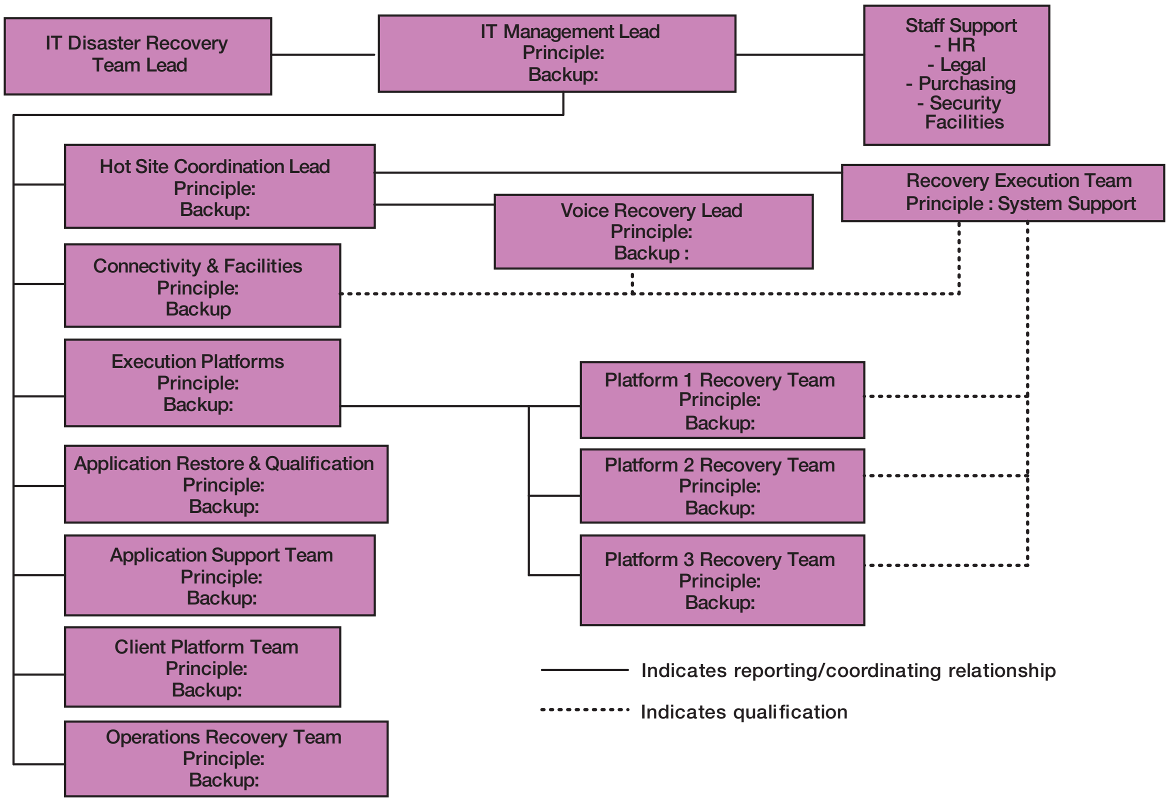
A disaster recovery program is more than just how to restore systems and data. The plan must include disaster identification, notification and coordination processes, communication plans, alternate computing facilities management, processes to return to normal operations, and DR plan testing and maintenance procedures. It must be a functional plan that addresses all of the processes required to restore technology and it must have a defined owner responsible for maintenance of the plan on an ongoing basis. A disaster response team must be identified and at the ready.

When developing the plan, it is important to determine the priority order of restoration across infrastructure and systems. One of the inputs to determining this is pre-requisite technology (e.g., the network must be restored before applications that rely on networked communications are restored.) A second input is the required level of uptime for each system. Systems requiring 24/7/365 uptime will need to be restored before those that don't have such stringent uptime requirements. Another factor to consider is the sustainability of the defined workarounds (i.e., how long can the manual workaround realistically suffice without causing bigger problems such as unmanageable backlogs, etc.). The person developing the DR plan must collect this information about all technology elements, perform a triage activity, and resolve any conflicts in the case of systems with dependencies or the same uptime requirements or conflicting priorities, and then determine the overall order of restoration required and document it in the plan. This information should be communicated back to the business area system owners so everyone is aligned with the planned order of restoration in the case of a disaster. This is important because recovery time expectations must be managed. Business area system owners whose systems are lower in recovery order must understand this fact and the drivers for that order.

DISASTER RESPONSE TEAM

The disaster response team must be identified ahead

Figure 2:
Example DR team organization.


IT Disaster Recovery Team Lead
IT Management Lead Principle: Backup:
Staff Support - HR - Legal - Purchasing - Security Facilities
Hot Site Coordination Lead Principle: Backup:
Recovery Execution Team Principle : System Support
Voice Recovery Lead Principle: Backup :
Connectivity & Facilities Principle: Backup
Execution Platforms Principle: Backup:
Platform 1 Recovery Team Principle: Backup:
Application Restore & Qualification Principle: Backup:
Platform 2 Recovery Team Principle: Backup:
Application Support Team Principle: Backup:
Platform 3 Recovery Team Principle: Backup:
Client Platform Team Principle: Backup:
Indicates reporting/coordinating relationship
Indicates qualification
Operations Recovery Team Principle: Backup:

of time. Roles, responsibilities, and backups must be defined, documented, and understood. Figure 2 shows an example DR Team organization.

Typical roles and responsibilities for personnel involved in DR are as follows.

DR Team Lead

The team leader's role and responsibilities include the following:

- Facilitates the disaster recovery process
- Ensures the workability of the plan by working through assigned teams
- Maintains and distributes the final copy of the plan
- Conducts impact studies
- Develops recovery strategies and response procedures
- Coordinates testing
- Monitors team response in actual disaster situations.

IT Management Lead

The IT management leader's role and responsibilities include the following:

- Assembles team leaders at the command center
- Places hot site on "ALERT" and makes formal disaster declaration
- Monitors the initial assessment activities
- Makes decision, based on initial assessment, to activate the DRP and subsequent recovery teams
- Monitors the hot site recovery and the home site restoration efforts
- Establishes and ensures the receipt of updates from the hot site coordination team lead on a regular basis
- Keeps senior management informed of the progress of the recovery effort
- Facilitates planning for return to a new or repaired facility.

Hot Site Coordination Lead

The hot site coordination leader's role and responsibilities include the following:

- Assembles hot site coordination team members at the command center
- Briefs, organizes, schedules, and mobilizes all subordinate recovery teams
- Oversees the preparation and restoration activities of all hot site environments
- Coordinates the identification, retrieval, and distribution of all off-site disaster recovery backup tapes and vital records
- Updates the IT management lead of restoration progress on a regular basis
- Receives and responds to restoration progress reports from all associated recovery teams
- Assists with planning for return to a new or repaired

facility.

Platform Recovery Team(s)

The platform recovery team's role and responsibilities include:

- Confirms the given platform (e.g., Unix, Windows, etc.) required hardware inventory at the hot site
- Updates the execution platforms lead on a regular basis
- Oversees and verifies the proper restoration of the given platform environment
- Ensures the execution of any required qualification for the given platform.

Application Restore And Qualification Team

The application restore and qualification team's role and responsibilities include:

- Coordinates recovery of applications in accordance with enterprise recovery prioritizations
- Verifies the integrity and accuracy of the restored critical application files
- Determines and coordinates the steps necessary to update and synchronize the restored files to their status as of the disaster occurrence
- Determines status of work-in-process at the time of the interruption
- Provides centralized coordination for all departmental unit concerns and processing requests
- Provides application-related assistance and staffing, if needed, to the other teams during the recovery period
- Communicates ongoing application changes to the computer operations team for evaluation of the impact on the contracted hot site recovery location
- Serves as the liaison between the IT organization and the application support teams for the recovery efforts
- Ensures the execution of any required application qualification.

Connectivity And Facilities Team

The role and responsibilities of the connectivity and facilities team include the following:

- Provides guidance and oversight to the voice recovery team
- Provides guidance and oversight to the recovery execution team in relation to connectivity restoration
- Ensures the completion of any required platform qualification
- Provides regular updates on progress of voice and connectivity recovery activities to the IT management team
- Assists in the planning for return to a new or repaired facility.

Execution Platforms Team

The role and responsibilities of the execution platforms team include the following:

- Coordinates the activities of the platform-specific recovery teams
- Reports the status of recovery activities to the IT management lead
- Assists in the planning for return to a new or repaired facility.

Client Platform Team

The client platform team's role and responsibilities include the following:

- Coordinates the acquisition of client device components as needed to recover and return to normal state
- Reports the status of recovery activities to the IT management lead
- Assists in the planning for return to a new or repaired facility.

Recovery Execution Team

The recovery execution team's role and responsibilities include the following:

- Obtains the appropriate backup tapes from the hot site coordination team
- Performs the restoration of the specific platform environments
- Reports the status of recovery activities to the hot site coordination lead
- Works with the platform recovery teams to ensure proper restoration.

Application Support Lead

The application support lead's role and responsibilities include the following:

- Coordinates the activities of the application support teams to enable end user problem resolution and assistance throughout the recovery period
- Maintains communications with end users.

Voice Operations Team

The role and responsibilities of the voice operations team include the following:

- Provides the necessary voice operations support for the initial and ongoing needs of the recovery effort
- Provides the operational support required to generate and maintain the voice hardware and system software needed during recovery
- Establishes and maintains a voice communications network capability for the critical internal and external user groups.

Operations Recovery Team

The operations recovery team's role and responsibilities include the following:

- Provides centralized coordination for all help desk requests
- Provides end user problem resolution and assistance throughout the recovery period
- Maintains communications with end users
- Communicates the prepared disaster statement
- Coordinates the setup and staffing of required operations at the hot site.

RECOVERY FACILITIES

The type of facility required for the DR operation must also be determined based on business requirements. A hot site is needed if fast recovery of data and connectivity is required and taking the time to actually rebuild the technology platform prior to recovery is not feasible. In the case of a hot site, hardware will already be on hand and mobile computing resources and desk space for critical staff are available. The network is designed to be able to quickly connect all unaffected systems to the hot site and telecommunications carriers are prepared to switch those capabilities to the hot site. The hot site is typically provided by a third-party service provider contracted by IT and provides these services on a subscription basis, governed by a contract. The subscription also typically covers periodic drilling of the DR plan using the hot site. Some corporations choose to designate one of their own locations as a hot site for the others; however, these locations must also be tested and drilled.

A cold site is used for build and recovery of data and connectivity in a situation where time is not as critical. Many DR plans use a hot site for immediate recovery of business critical systems and then move to a cold site to rebuild lower priority platforms. A cold site is much less expensive than a hot site, because it is really only providing a facility. This space must be outfitted at the time of need by the subscribing company, and the arrangement should include quick-ship agreements with vendors because there is no equipment on hand. This option is certainly less costly but if used solely, significantly slows recovery time.

Whichever type of recovery facility is selected, choose a location that will likely not be affected by the same disaster, but that is still within a reasonable travel distance and time. Storage location for backups must be accessible within a reasonable time and effort and/or an arrangement in place for quick-ship to the recovery site. With respect to storage of the DR plan, keep a copy of the plan in several locations (e.g., company facility, recovery site, in possession of the DR lead.)

MAINTAINING THE DISASTER RECOVERY PLAN

Once developed, the DR capability must be tested initially and then drilled periodically. Drills typically identify snags, which should result in updates to the DR plan. A drill doesn't always have to be a full-blown simulation of the actual process—there can be segmented drills (for selected portions of the technology/selected systems) at the DR location, and in some cases, a "conference room" drill (one in which the process is walked through procedurally) can suffice. It is not recommended to ONLY perform these abbreviated options, however. Hot site contracts typically include several drills per year, of which the company should take advantage.

Some common (and easily avoidable) mistakes with respect to DR execution are such things as missing or forgotten software product keys, outdated contact information for key personnel or service providers/vendors, not assigning backups for DR team roles, and blank or corrupt backup tapes. One of the most frustrating mishaps is discovering that the DR plan was maintained in electronic form only and is, therefore, not available when needed.

One person should be assigned the overall responsibility for maintenance of the DR plan (normally the DR lead). The plan should be updated when drill results dictate a change, when there are system implementations or retirement, and when significant changes are made to systems that would affect their recovery method. The DR lead must maintain the plan master copy and ensure that all copies of the plan are the most recent version and that old versions are destroyed. Additionally, the DR lead must maintain any sensitive combinations, passwords, etc. that will be required during DR but cannot be put into the plan.

DEVELOPING A DISASTER RECOVERY PLAN

If you do not have a DR plan in your company, it is advisable to develop one. Steps to do so are as follows:

- **Stakeholder support.** Identify management stakeholders and gain support and funding by creating a business case for why it is needed. This can sometimes be a tough sell because DR is similar to insurance and it is sometimes difficult to imagine needing such a thing. Be persistent.
- **Project requirements.** After approval and support to proceed, gather uptime and recovery time requirements and technical requirements and constraints from the business and from IT subject matter experts.
- **Project team.** Form a team to define a plan to balance the recovery time requirements with relative priority and available resources, and use a risk-based approach to determine the overall recovery order.
- **Gap analysis and remediation.** Identify any gaps and remediate them.
- **Disaster recovery plan.** Draft the plan, review with stakeholders, finalize the plan, and conduct a drill.

Revise the plan as required.

CONCLUSION

This article discusses disaster recovery, business continuity, and contingency planning and how understanding and implementing these measures are important for the integrity and compliance of the systems in today's environment of technology and automation.

System owners and technology professionals should understand how these plans should be developed and when and how to exercise them. System owners should have a DR plan in place and all team roles and responsibilities should be clearly defined. A company should have a functional plan that addresses all of the processes required to restore technology, an individual responsible for that plan, and a disaster response team at the ready.

REFERENCE

1. FDA, HHS, Code of Federal Regulations, Title 21—Food And Drugs, Chapter I—Food And Drug Administration, Department Of Health And Human Services, Subchapter A—General, Part 11, Electronic Records; Electronic Signatures. GXP

ARTICLE ACRONYM LISTING

BC	Business Continuity
CP	Contingency Plan
DR	Disaster Recovery
EBC	Enterprise Business Continuity

ABOUT THE AUTHOR

Barbara Nollau, column coordinator, is director of quality services at Abbott Vascular. She is responsible for validations, reliability engineering, supplier quality, microbiology, and document management at Abbott Vascular. Ms. Nollau has 25 years experience and increasing responsibility in pharmaceutical and medical device industries, spanning areas of manufacturing, quality assurance/compliance, and information services/information technology. Ms. Nollau can be reached at barbara.nollau@av.abbott.com.

Originally published in the Summer 2009 issue of *Journal of GXP Compliance*