

Understanding the need for Business Continuity Management and Disaster Recovery Planning

By Ed Tittel and Justin Korelc

Introduction

This paper is meant to provide an introduction to and a broad overview of the intertwined subjects of Business Continuity Management and Disaster Recovery Planning, commonly abbreviated BCM and DRP. As such, this material is probably most useful to those with little or no familiarity with these topics. Readers who fall into this category would be well served to read this document from start to finish. On the other hand, financial professionals with at least some familiarity with this subject matter should at least read the next section at a minimum, the sections entitled “Special BCM elements for accountants” and “Special DRP elements for accountants,” and then jump to the end of the paper to look over the annotated reading and resource list created to accompany this paper. That information should be of interest, and can lead readers to additional, more detailed references and resources.

Here’s a roadmap to the contents of this document:

- Introduction (what you’re reading right now)

- Coping with Business Interruption

- BCM and DRP Opportunities for Financial Professionals

- What is BCM?

 - Scoping and Planning BCM Projects

 - Business Organization Analysis

 - Assembling a BCM Planning Team

 - Requirements: Resources, Legal, and Regulatory

 - Assessing Business Impact

 - Establishing a Continuity Strategy

 - BCM Documentation Elements

 - Special BCM Elements for Accountants

- What is DRP?

 - Classifying and Understanding Disaster

 - Establishing a Recovery Strategy

 - Developing a Recovery Plan

 - Training for and Documenting DRP

 - Testing and Maintaining DRP

 - Checklist Test

 - Structured Walkthrough

 - Simulation Test

 - Parallel Test

 - Full Interruption Test

 - Maintenance Tasks

 - Special DRP Elements for Accountants

 - Pointers to Reading, Certifications, and Other Resources for DRP

Coping with Business Interruption

Despite our best efforts and precautions, disasters of all kind eventually strike an organization, usually unanticipated and unannounced. Natural disasters (i.e., hurricanes and earthquakes) and other events (i.e., building fires and broken plumbing) can threaten the very existence of an organization. Well-prepared organizations establish plans, procedures and protocols to mitigate the effects any form of disaster may have on continuing operations and help facilitate a speedy return to working order. Continuity and recovery planning are two separate procedures of reparation to restore and recover critical business operations in the event of such disasters.

As we become increasingly reliant on information technologies and business-critical information, protecting these systems and providing for their continuity and recovery becomes an even greater priority. The importance of protecting irreplaceable data cannot be over-emphasized. With so much business and so many businesses relying heavily on information and information systems there is no viable rationale for going without these plans. The statistical data is eye-opening: many large companies spend between 2-4% of their IT budgets on disaster recovery planning (to avoid larger losses). A study conducted by McGladrey and Pullen, LLP shows that among companies that suffer major losses to computerized data, 43% never reopen for business and another 51% (enduring outages longer than 10 days in duration) shutdown within two years. Only a marginal 6% actually survive the long-term. Poor or neglected planning is costly—don't become one of these statistical references.

Although Business Continuity Management (BCM) and Disaster Recovery Planning (DRP) show some overlap in certain logistical ways, the two completely differ in practice, protocol and purpose. The crucial distinction is given away by the acronyms—one includes *continuity* or the continuation of business, whereas the other utilizes *recovery* to denote healing, saving or returning to an original state. These differences and distinctions will be explained further in the passages that follow.

BCM and DRP Opportunities for Financial Professionals

A decent working understanding of BCM and DRP, which this document should provide if you don't already possess such knowledge, should inform financial professionals that they can play important roles in the planning, maintenance, audit, and execution of business continuity and disaster recovery plans. It should be patently obvious that access to financial information, payables and receivables, and other key information, accounts, and activity related to any organization's normal operations will be crucial whether that organization seeks to maintain continuity (which is where BCM comes into play) or to re-establish normal working conditions as soon as possible in the wake of some serious business interruption (which is where DRP enters the picture).

Financial professionals should not let the IT-intensive focus normally associated with BCM distract them from the realization that uninterrupted access to financial data, systems, and activities is just as important to business continuity as are the technical information technologies that so often support such things. Likewise for DRP, restoring access to financial data, systems, and activities is every bit as important to re-establishing normal business operations as are the information technologies, networks, services, applications, and so forth, so often used to interact with them.

What kind of opportunities does this present to savvy financial professionals? First and foremost, it argues strongly that they must be involved in all phases of BCM and DRP activity, including initial research and analysis, development and formulation of business continuity and disaster recovery plans, as well as subsequent auditing, testing, and maintenance of such plans as they change and evolve to reflect changing circumstances, business goals, macroeconomic trends and other phenomena. Whether a CPA operates within a private practice, supports the financial interests of a public or private firm or organization, or works for a large public accounting or consulting firm, BCM and DRP offer profound opportunities for involvement both as planning and implementation activities get underway, and throughout the course of the normal monthly, quarterly, and annual business cycles.

For those who may be inclined to question the value of BCM or DRP, consider this: both business continuity and disaster recovery planning are becoming integral to demonstrating prudent financial practices and procedures. This is particularly true for firms that may be seeking outside capital, where such plans may even be required to qualify for loans or lines of credit, and becomes even more important publicly-held companies or those seeking to go public, where such plans often appear on the checklists of institutional and individual investors and analysts as they seek to separate potential winners and losers in the marketplace.

What is BCM?

Business Continuity Management (BCM) is an interdisciplinary concept used to create, establish, validate and maintain a practiced logistical plan (aptly called the *business recovery plan*), which defines, describes and details how an organization will continue partially or completely interrupted critical functions within some predetermined timeframe. The BCM methodology scales to organizations of any size and complexity, with roots in regulated industries and any type of organization that wishes to ensure its own longevity in the face of adversity. Finally, BCM outlines the *who, what, when* and *how* of a continuity plan; reduces disruption of vital business operations; and addresses a broad range of events encompassing both natural and unnatural disasters.

A Call for Clarity

Continuity is defined as: an uninterrupted connection or union; the property of a continuous connectivity over a period of time; and the absence of interruption and a succession of intimately united parts. In these definitions the common denominator is an *interruption* to connectivity, operation or service.

In most cases, BCM goes into effect following an environmental disaster or some kind of enduring disruption. A principle tenet driving BCM, is *risk management*—assessing the likelihood that vulnerability will be exploited and thereby determining an appropriate response, course of action, and allocation of resources to counter an actual or threatened interruption. The crucial point of emphasis is that BCM isn't architected to *prevent* every event with the potential to negatively impact operations from affecting an organization—an improbable, impractical and impossible task. Instead, BCM is designed to *limit* the damage extending from natural and man-made disasters or any other disruption that negatively impacts business. Stated another way, BCM assesses the risk that such occurrences pose to organizational processes, minimizes those risks to business functionality, and establishes a course of action to support continued operations should such an event actually occur.

In simpler terms, BCM involves determining how to continue business operations in the wake of both man-made and natural disasters. Localized incidents (such as arson, theft, vandalism, terrorism, extended power outages, and so forth), regional incidents (such as earthquakes, floods, tornadoes, wildfires, and so on) and national incidents (such as economic downturns, supply shortages, pandemic illness, etc.) are all considered and factored into the plan. BCM may be part of a distinct enterprise-level learning effort seeking to reduce operational risks associated with lax information management controls, and integrated with practices that improve information security and corporate reputation risk management practices.

Scoping and Planning BCM Projects

Completion of the BCM plan should result in a formal printed manual available for reference before, during and after business disruption occurs, as part of the project deliverables. The purpose the manual (or in some cases, the other set of documentation) is to reduce stakeholder impacts drelated to the scope of a disruption (*who* and *what* is affected) and the duration of the disruption (*how bad* and *how long*).

The focus of BCM falls primarily on continuing and maintaining business operations with reduced or restrictive infrastructure capabilities, functionality, and resources. Where an organization remains able to sustain mission-critical tasks following a disaster, or re-establishes at least reduced operational capacity quickly thereafter. BCM plans should include provisions to enable such operations to continue until a complete recovery has been affected.

Business Organization Analysis

Analyzing the business organization and its entire operational footprint is instrumental to developing a proper continuity strategy. This begins with identifying mission-critical functions throughout the organizational landscape, including agency functions (interdependent services performed by agency processes and sub-processes), enterprise functions (services dependent upon agency-level functions) and processes (series of actions or operations that implement functions).

Identifying mission-critical functions can be a tedious task, and no two organizations will follow the same process or end up with the same list. When identifying mission-critical functions, the following should be considered:

- Functions that support the organization's primary mission statement
- Functions that support other agencies' mission critical functions
- Functions that must be recovered immediately and quickly
- Functions that have a high-dollar value
- Functions that have high client/customer impact
- Functions with political implications or ramifications
- Functions with legal requirements or liabilities

An executive Business Impact Analysis (BIA) tool can facilitate this process, helping planners and organizers understand the effects and impacts of interruption on the viability and vitality of operations and critical business functions, especially financial activities, including maintaining collections, processing payments, operating a supply chain, handling payroll and so forth. BIA is the backbone of the BCM planning process but cannot stand alone without full approval, backing and support from the highest level managers.

Risk analysis and Risk assessment are additional processes which support the BCM planning process. Risk *analysis* involves identifying probable threats and associated threat value to an organization and its assets and analyzing related vulnerability. Risk *assessment* evaluates existing environmental and physical controls and security, followed-up by assessing their adequacy relative to potential threat.

Assembling a BCM Planning Team

The goal of BCM planners is to advise, create and implement a combination of policies, procedures and processes to minimize disruptive or negative impacts to routine business operations. The composition of the project team is critical to the BCM planning process and the development of a comprehensive and effective team. Candidate selections should strike a balance between technical skill, business process knowledge, distinct leadership traits, team orientation and positive attitude. The following categories of expertise should be represented:

- Team leaders
- Technical members
- Business process experts
- Support personnel

Consider each member as an individual element specialized in their own respective capacities. The team lead is tasked with ensuring that skills and talents are well-placed and well-utilized. For example, when conducting lengthy business process interviews it's necessary to select a portion of the team most familiar with those processes, who can then report their findings summarily to the remaining team.

Business process team members require expertise—you don't want disaster recovery to be a crash-course in business process. BCM planning teams should utilize expert insight to determine effective ways to protect critical processes from risk. After conducting an organizational risk assessment to identify critical processes, consult with process owners to locate individuals with solid understanding of these processes.

Technological experts include team members with specialized skills in keeping systems online and operational on a daily basis. The BCM planning team therefore requires representation from each of the major technology groups in your organization—database and system administrators, storage engineers, security professionals, application specialists, backup technicians and customer support personnel.

Support team members are the personnel that support the business process and technical members of the BCM planning task force. These individuals may include general counsel (handles legal and regulatory issues), public affairs representatives (the public mouthpiece for the organization), administrative assistants (help document and administrate the BCM plan) and procurement specialists (who bring supply-chain

knowledge to the table). As with other elements of the BCM planning process, the exact composition of the BCM planning team will be organization-specific.

Requirements: Due Diligence, Governance, and Plan Execution

Another crucial tie-in to the BCP strategy involves prudent financial practices involved with business continuity and disaster recovery procedures. Continuity and recovery, along with information security concerns, are continuing hot topics on Capitol Hill and within various standards bodies, and the concerns over these issues has given rise to regulations, best practices and procedures that tie financial accounting and reporting to BCM and DRP. For example, while Sarbanes-Oxley does not specifically address BCM or DRP, most auditors consider a viable Business Continuity and Disaster Recovery plan, as an important component of internal control. The BCM team lead is primarily responsible for ensuring that all members are briefed and thoroughly understand all applicable laws and regulations governing BCM and DRP.

It also behooves financial professionals to research and raise issues related to current and available forms of insurance as part of the BCP (and DRP) processes. This can include such insurance vehicles as:

- Business insurance: many general business insurance policies devote specific sections to coverage of losses related to business interruption, whether or not it's related to a disaster or other causes. It's important to review this coverage, and to become acquainted with areas where coverage is available, and areas where risks of loss must be offset through other insurance or other means of mitigation.
- Business recovery or continuity insurance: available from both specialized and general insurers, this type of coverage may be used to offset business recovery expenses related to equipment breakdowns, infrastructure failures, and other potential causes of business interruption
- Loss or business interruption insurance: a type of special insurance that provides protection against the loss of profits resulting from an interruption in commercial activities due to some specific event

Where insurance is available, cost can be weighed against risks during the various assessment phases described in the sections that follow. Because such coverage is usually stated in terms of definite costs and amounts, formal risk analysis is relatively easy, as long as the amount of related losses can be properly quantified.

Assessing Business Impact

Defining potential threats and documenting impact scenarios are the basis of business recovery planning. Over-planning for the most wide-reaching disaster or disruption is preferable to under-planning for much smaller-scale issues. In many cases, these smaller issues are merely elements in much larger or more complex disaster scenarios. Worst-case scenario strategizing encompasses all critical business functions and the worst possible outcome from any potential threat.

A comprehensive business continuity plan should also document additional impact scenarios where an organization encompasses more than one building. Other, more specific impact scenarios (i.e., considerations for single-floor disasters with temporary or permanent consequences) should also be documented.

Establishing a Continuity Strategy

The development process for a business continuity plan consists of five essential phases:

1. Analysis
2. Design
3. Testing
4. Implementation
5. Maintenance

Many other considerations beyond the scope of this document are not included but should be accounted for in the final process. Other considerations include the risk identification matrix, roles and responsibilities, resource reallocation considerations and other skill matrices for larger organizational footprints.

BCM Documentation Elements

A simple BCM manual might be printed and stored safely away from the primary work location—thus, beyond the reach of a site-specific disaster. This manual should contain contact names, phone numbers and addresses for crisis management staff. General staff, current client lists, and vendor contacts should also be included. Locations for back-up storage media, insurance contract copies and other organizational survival necessities should also be included.

More complex BCM documentation might outline a secondary work site, technical requirements, technological readiness, regulatory reporting requirements, work recovery measures and the means to reestablish damaged or destroyed physical records. Other items include methods for establishing a new supply chain and the means to establish new production facilities (where applicable). An organization should ensure that their BCM manual is practical to use during a crisis.

Special BCM Elements for Accountants

When it comes to developing, implementing, or maintaining a business continuity plan, the roles for financial information and activity and the accounting professionals who are typically responsible for them cannot be overemphasized. Although professionals from Information Technology and Operations invariably play key roles in the BCM planning process, financial professional with accounting knowledge and responsibilities must also be deeply involved in this process as well, if only because a company's or organization's continued (or minimally interrupted) financial activity is usually a top priority in ensuring business continuity. This explains why accountants, CFOs, and financial analysts must not only be aware of BCM activities, plans, documents, and tests, but also as actively involved in these functions as they can manage.

In supporting their organization's BCM planning efforts, or advising clients with respect to BCM, CPAs can apply the AICPA's Trust Services Principles and Criteria, to apply a set of professional assurance and recovery services based on a common framework that may be used to address the risks and opportunities inherent to use of and dependence on information technology (IT). This framework and its criteria should help financial professionals offer input and advice on matters related to IT security, availability, processing

integrity, online privacy, and confidentiality. It should also enable financial professionals to help firms and organizations assess business opportunities and risks related to use of third-party service providers, new, complex business technologies and e-commerce, including issues related to trustworthiness, including reliability, privacy, and security.

The primary impetus is to make sure that business entities and operations are attuned to the risks that their environments can pose, and equipped with proper controls to address such risks. To that end, AICPA has developed both SysTrust and WebTrust as specific services that implement these principles and criteria, and are designed to help financial professionals deliver advisory services or assurance on systems reliability (SysTrust) and for matters related to e-commerce (WebTrust).

Another area where financial professionals can play an important role related to BCM and/or DRP—is in the valuation of losses and handling of claims related to business continuity or disaster recovery events. CPAs generally play important roles across the board when such claims are filed: they will often be involved in assessing inventory, recent activity, and current conditions upon which an organization’s claims will be based. On the receiving end, CPAs will likely work at the insurer’s behest to analyze the basis for such claims, and help decide on their applicability and merit. And finally, if and when claims-related litigation should take place, CPAs specializing in litigation support and valuation may get involved to examine the filings and contentions of all parties involved, and to voice opinions on their validity, merit, and applicability to help jurists and juries to decide such cases.

What is DRP?

Disaster Recovery Planning (DRP) describes the processes, policies, and procedures behind the *recovery* of mission-critical functions necessary for the resumption and normal functioning of business and/or day-to-day operations. DRP establishes order where chaotic events reign over interrupted business functions. It also serves as a unifying basis for recovery strategy when tensions run high and mental clarity or cool-headedness runs low.

Recovering from disaster scenarios involves restoring access to data (such as client records, item inventories, financial information, hardware and software components), communications (including incoming and outgoing network connections, plus phone and fax systems), workspaces (such as computing environments, compartmentalized departments) and business operations and processes. A Disaster Recovery Plan represents a thorough and complete set of procedures, processes, and protocols for recovering from any kind of disaster as quickly and painlessly as circumstances will allow.

A Call for Clarity

Recovery (in this sense) is the ability to recuperate from the loss of a complete site and the protocols and associated procedures for returning lost computer systems, data transactions and business processes to working order.

By now you should understand that BCM and DRP represent different phases of the same process. BCM helps ensure continuance of disrupted business functions; DRP helps manage and drive the restoration of interrupted infrastructure elements necessary to support business operations. In such a scenario, BCM merely picks up the fumbled ball and keeps running, where Disaster Recovery helps bring players back into

the game after they sustain an injury . Remember, BCM happens first and if its efforts fail (or the sustained damage toll is too prolonged or costly) DRP follows-up to fill the gap.

Classifying and Understanding Disaster

Envision the circumstances where it's necessary to implement recovery measures: a tornado devastates a primary or critical operating facility; fire consumes a main processing center; or terrorist activity denies passage to a company campus or surrounding territory. Disasters will strike your organization—it's only a matter of time and severity. Organizations want to survive the negative impacts of a disaster and to continue serving and servicing their customers in an efficient, reliable manner.

Disaster comes packaged in many forms depending on regional location, geography, topography and other circumstances. Natural disasters include violent geologic or weather-related events such as earthquakes, fires, floods, hurricanes, thunderstorms tornados and tsunamis. Man-made disasters include arson, power outages, infrastructure failures, utility outages, theft, vandalism and acts of terrorism. These events represent a good starting point, but by no means represent an exhaustive list. Each organization needs to take into consideration only those elements that are relevant to their specific situations and include any of those left unmentioned.

Establishing a Recovery Strategy

DRP begins with a complete assessment of the IT network—including connectivity, hardware and software. A thorough follow-up review identifies potential problems and threats and the recovery plan is drafted from these findings. The resultant product is a “living” document—one that grows and changes in scale and scope as the organization evolves—that establishes original working order in the wake of a catastrophe that halts business operations.

Before establishing any disaster recovery (DR) strategy, the DRP team should first consult the organization's continuity plan. This will indicate key metrics for Recovery Point Objectives (RPOs), criteria that must be satisfied to meet operational recovery requirements in terms of how long data ages between the moment of failure and when the next valid updates can occur thereafter; and Recovery Time Objectives (RTOs), criteria that must be met to satisfy maximum acceptable time periods for various business processes, such as payroll processing, managing payables and receivables, and order processing. Most important, the metrics specified for these and any other business processes must be mapped into the IT infrastructure and computer systems needed to support or provide them, along with the data they require to function as expected.

Once RTO and RPO metrics are mapped, the DR team can properly determine the most suitable recovery strategy for each system. RTO defines deliverable timeframes for bringing critical functions back online and into fully operational states. RPO describes the amount of data lost as measured over time (such as “the last available copy of data is X hours old,” so that “RPO equals X hours”).

Developing a Recovery Plan

The DRP should be established in such a way that it runs on autopilot minimizing the need for decision-making activities during critical downtimes—neither the ideal time nor place for strategic planning or critical decision-making . Support personnel should also be well-trained, to understand their capacities,

duties and responsibilities in the wake of disaster. This will allow them to operate in a near automated state, enabling them to react to the situation with which they are presented, though critical thinking skills will still be required to handle situational variation.

Established business unit priorities pave the path to drafting an organizational DRP. It also helps to have a good idea of what alternative recovery sites exist for your organization. The DRP should be designed to initiate automatically and operate initially with on-scene first responders until remaining team members have arrived on site. Since the DRP logically flows from the BCM plan, it mirrors the prioritization tasks the BCM team performs during BIA and any resulting documentation serves as the basis for such tasks.

Training for and Documenting DRP

Clearly the DR plan should contain comprehensive instructions for DR support personnel to immediately act upon when- and wherever necessary. Instructive elements vary according to the nature of events, response personnel and pre-evacuation timeframes, therefore it is vital that all relevant DR personnel are uniformly provided with accurate, timely documentation. There will be variation among the level of training provided to individual support staff, which depends upon their roles in the recovery effort and their positions within the company or organization to which they belong.

As with in BCM, it is imperative that all personnel involved in the recovery process receive adequate training. Levels of provided training will vary according to individual roles and responsibilities so that several dimensions should be considered, including:

- Orientation training for new hires
- Initial training for newly-tasked DRP personnel (first-timers)
- Refresher courses and live exercises for recovery team elements
- Debriefing training for all other employees

Every part of the DRP process should be fully documented and released on a “need-to-know” basis. DRP documentation is extremely sensitive and all participating parties should be fully aware and understand their capacities within the process, and understand the need to keep this information carefully cloistered within the disaster recovery team. This documentation should include:

- Executive summary
- Departmental strategy
- Technical guides
- Individual checklists
- Full copies of DRP

Accurate, custom-tailored and timely documentation is especially important, and participants should be required to refresh their roles, responsibilities, and routines in the DRP process on a regular basis. These

individuals should refer to their departmentalized DR procedures, and be guided by action checklists and high-level coordination procedures to ensure speedy, effective infrastructure restoration.

Testing and Maintaining DRP

Testing and validating procedures and processes are essential to a properly functioning DR plan, and should be retested and revalidated continually. Again, both BCM and DRP processes produce “live” documents that must adapt and evolve to meet changing business needs. There are several approaches to testing and validating DRP that are described accordingly below.

Checklist Test

Among the simpler methods is the checklist test. DRP checklist copies are distributed to members of the DR team for thorough review to ensure personnel awareness, procedural review and replacement for members of the team that are no longer available.

Structured Walkthrough

This testing procedure (also called a *table-top exercise*) goes a step further and involves a war room role-play exercise. A test moderator submits an exact scenario who presents details and specifics at the team meeting, where team members then review their DRPs and discuss appropriate responses.

Simulation Test

Another incremental step presents DRP teams with a scenario where they are asked to formulate a response to simulated disaster conditions. However, in this testing phase team members conduct actual exercises and test proposed measures, which may involve the interruption of business activity.

Parallel Test

The next level in testing involves the actual relocation of supportive DRP personnel to an alternate recovery site to conduct exercises and implement procedures. Relocated employees perform their DR responsibilities as if it were an actual disaster scenario, without disruption to the existing business.

Full-interruption Test

Finally, the *full-interruption test* mirrors the *parallel test* practice and involves full shutdown of operations at the primary site and a fully-operational shift to the alternate recovery site. Clearly this is an intrusive testing methodology that is difficult to orchestrate and often encounters resistance.

Maintenance Tasks

As a live body of documentation, DRP requires constant maintenance to ensure accurate responses, appropriate procedures and adaptive processes to restore working order. Many changes and maintenance tasks are exposed through adequate and proper testing methodologies. Minor changes may be issued through basic contact (e.g., phone, email) whereas major changes require face-to-face meetings and full DR team coordination. Again, the DR team should refer to the established BCM plan as a template for further recovery efforts.

Special DRP Elements for Accountants

As with BCM, financial professionals, CFOs, and other staff members with financial responsibility should be involved in all phases of DRP activity: design, planning, testing and maintenance to be sure, and also most

certainly in the event of any actual disaster that results in invocation of DR plans, processes, and procedures. Here again, because access to financial information and systems is such a key component for continued, proper function of businesses and organizations of all kinds, rapid restoration of access to such information, and resumption of all key financially significant line-of-business and back office functions should be at the top of the priority list when recovering from a disaster. Only by serious, dedicated involvement in the disaster recovery process can financial staff ensure that their needs and priorities are properly considered, handled, and ultimately satisfied.

As in our earlier discussion under a similar heading in the BCP section of this paper, licensed CPAs and CPA firms should read and consider the AICPA's own Trust Services information to help guide the services relevant to DRP that they offer, and the types of advice and assurance that such services can cover. Without repeating the information provided in that section (and in the AICPA's other documents on Trust Services) it suffices to say that CPAs can (and should) get involved in researching and preparing, auditing and maintaining, and testing disaster recovery plans. They can also play important roles for various players in filing (on behalf of policyholders), evaluating (on behalf of insurers or underwriters), or analyzing (on behalf of the court, plaintiffs, or defendants) claims filed to recover losses related to disasters.

Pointers to Reading, Certifications, and Other BCM and DRP Resources

In our companion reading list, you'll find discussions of all kinds of useful information related to BCM and DRP, including:

- Courses and training from both government and academia. On the government side, the most notable offerings come from the Federal Emergency Management Agency (FEMA), which operates an Emergency Management Institute that is home to all kinds of training materials, plus courses and features programs on a wide variety of BCM and DRP topics. On the academic side, we make mention of a program from the University of Illinois at Chicago entitled "Emergency Management and Continuity Planning" and indicate numerous other academic institutions where similar programs are offered, and provide a link to college options documented by a university professor who specializes in this subject area.
- Certification Programs: These include multi-level credentials from such parent organizations as DRI International, also known as The Institute for Continuity Management, and the Business Continuity Management Institute, or BCMI, that include business continuity and disaster recovery topics, as well as emergency management topics as well.
- AICPA Trust Services Principles and Criteria: This is part of the AICPA's coverage of System Security and Reliability\ . Trust Services are best understood as a set of professional assurance and advisory services built around a common framework (or a core set of principles and criteria) by which risks and opportunities in information technology (IT) may be addressed. AICPA has compiled numerous documents in this area, including a general overview, analysis of the effects of a third-party service provider, a FAQ that addresses common questions about generally accepted privacy principles for specific engagements, and so forth. In addition, AICPA has defined two specific services in this realm: WebTrust, which applies the Trust Services principles and criteria to electronic commerce,

and SysTrust, which applies those same principles and criteria to system reliability. Validation audit criteria and certification authority coverage is also provided on the WebTrust side. For more information, visit the AICPA IT Center website at <http://infotech.aicpa.org/Resources/System+Security+and+Reliability/System+Reliability/Trust+Services/>.

- Books and Other Useful Materials: This part provides capsule summaries of ten current and relevant book-length publications on BCM and DRP, most in print (one on CD-ROM). Readers looking for more details on BCP and/or DRP concepts, terminology, practices, and procedures should find these references of at least potential interest as they conduct such a search.

Operations (COOP) Specialist, and BS24999 Specialist. There is also an entry-level Associate Continuity Manager (ACM) credential, and a Certified Continuity Auditor (CCA) credential for those who specialise in either internal or external BCP audits. Other, well-known training companies such as Learning Tree, Mile2, OnlineContinuity.com, Kingsbridge Disaster Recovery, among numerous others, also offer DRP and BCP courses, sometimes with and sometimes without their own “private-label” certifications.

AICPA Trust Services Principles and Criteria

The AICPA has itself devoted substantial time and resources to addressing a set of professional assurance and advisory services built around a core set of principles and criteria known as Trust Services, designed to address both the risks and opportunities posed by the use of information technology (IT) in modern firms and organizations. These originate from the Assurance Services Executive Committee of the AICPA, and include coverage of both e-commerce systems and activities online (WebTrust) as well as inherent system reliability issues (SysTrust). Those interested in understanding this realm of services must quickly recognize that Trust Services has immediate and beneficial applications in the areas of BCP and DRP.

Key documents for AICPA Trust Services include the following:

- The AICPA [Trust Services](#) home page, which includes pointers to all other documents and items cited below.
- [Trust Services Principles and Criteria—An Overview](#): A description of the core principles and criteria upon which trust services rests, including illustrations, as it applies to security, availability, processing integrity, confidentiality, and privacy, where each of these five domains is subject to specific governing policies, communications, procedures, and monitoring requirements. This includes mention of specific performance and reporting standards as set for in the *Statement on Standards for Attestation Engagements (SSAE), No 10, Attestation Standards...* ([AICPA, Professional Standards, vol 1, AT sec. 101](#)). CPAs may offer strategic, diagnostic, implementation, and sustaining/managing services using Trust Services principles and criteria.
- [WebTrust](#) deals with situations where e-commerce components are involved, within the five domains to which the Trust Services themselves apply (security, availability, processing integrity, confidentiality, and privacy). Basic documents provide an overview of WebTrust services and their benefits to CPAs, marketing advice, a skills inventory, getting started, and a FAQ on WebTrust. More advanced documents cover the [impact of third party service providers](#) on WebTrust engagements, [extended validation audit criteria](#), and assessments of the adequacy and effectiveness of controls employed by [Certificate Authorities](#) (CAs).
- [SysTrust](#) addresses system reliability issues, within the five domains to which the Trust Services themselves apply (security, availability, processing integrity, confidentiality, and privacy).

Documents available include an overview, marketing advice, a skills inventory, getting started with SysTrust, and a general SysTrust FAQ.

Books and Other Useful Materials

Available from the AICPA Store (www.cpa2biz.com)

Risk Management - A CPAs Toolkit for a Changing Environment - Disaster Recovery and Business Continuity, by Anthony E. Davis, Esq.; Marcia Gordon, CPA; Robert H. Spencer, Ph.D. This fifty-two question in-depth survey available via download can be used to assemble and organize information regarding the firm's existing preparations, policies and procedures in the event of a disaster.

Disaster Recovery: A Guide to Financial Issues, Published by the AICPA. In this consumer resource booklet, you will find suggestions on steps to take immediately following a natural or man-made disaster, what to do in the initial weeks and months, and how to begin planning for the future. Specifically, find the following topics: restoring household stability, managing an injury or disability, financial decisions after a death, lawsuits and other settlements.

Management Accounting Guideline: Business Continuity Management (BCM), Published by the AICPA. This Management Accounting Guideline available for download has been designed to:

- Show how to define BCM and its essentials and processes;
- Identify the BCM-related roles of corporate managers and directors;
- Work through a BCM framework for developing and maintaining effective business continuity management processes;
- Show examples of leading BCM capabilities in practice.
- Present a step-by-step framework for developing and maintaining effective business continuity management processes;
- Provide an overview of the software applications available to support BCM planning and execution processes;
- Present examples of sound business continuity management capabilities in practice.

Additional Resources

Business Continuity and Disaster Recovery Planning for IT Professionals, by Susan Snedaker, Syngress, June 8, 2007, ISBN: 1597491721. A well known expert on IT project management applies her expertise to BCP/DRP, and delivers the goods in a straightforward, readable style. The book begins by putting BCP and DRP into the context of the kinds of interruptions and disasters that businesses typically face, then move readers step-by-step through the processes involved in planning for disaster, and in ensuring business continuity in the face of interruption or disaster. She also covers important financial aspects involved in business disruption and deals with accounting and accountability concerns in detail as well, particularly in the areas of risk assessment and business impact analysis.

Business Continuity Planning Methodology, by Akhtar Syed and Afsar Syed, Sentryx, November 2003, ISBN: 0973372508. This book provides a complete and thorough exploration into and explanation of the entire body of the Disaster Recovery Institute International (DRII) professional practices, with in-depth examples, illustrations and discussions of each topic. A complete and thorough reference book, especially for those tasked with designing or building business continuity or disaster recovery plans.

Business Continuity Planning: A Step-by-Step Guide with Planning Forms on CD-ROM, 3e, by Kenneth L. Fulmer, Rothstein Associates, October 2004, ISBN: 1931332215. A short, tightly focused book built around templates for creating a business continuity plan with explanations of the sequence of tasks and the background work involved in completing the planning forms provided on CD-ROM with this title. Not for seasoned BCP planners for whom this material should be quite familiar, but very helpful for IT and operations professionals who may find themselves tasked with designing and building a BCP, especially in small to medium sized organizations.

Business Continuity: Best Practices--World-Class Business Continuity Management, 2e, by Andrew Hiles, Rothstein Associates, December 2003, ISBN: 1931332223. This book covers topics of interest to both the Business Continuity Institute (BCI) and the Disaster Recovery Institute International (DRII, aka DRI). It takes a look at topics from a basic foundation level and in terms of how practitioners might best approach them, but functions primarily as a broad introduction with lots of pointers to more advanced and detailed materials than as a complete reference work on the subject matter. Might be a better general introduction to the subject matter than "The Backup Book" cited elsewhere in this reading list, but will probably come down to the individual buyer's taste and preferences.

Contingency Planning and Disaster Recovery: A Small Business Guide, by Donna R. Childs and Stefan Dietrich, Wiley, October 21, 2002, ISBN: 0471236136. A short (288 pp) but tightly focused and well-organized approach to helping small businesses prepare for contingencies and to implement effective, well-designed disaster recovery plans. Works well as a preventive measure in advance, but is also cited as a helpful tool for those recovering from disasters by readers who've been through them.

Disaster Recovery Planning: Preparing for the Unthinkable, 3e, by Jon William Toigo, Prentice Hall PTR, September 6, 2000, ISBN: 0130462829. Provides a well-researched and organized view of the subject matters for disaster recovery planning, and makes mention of software and products available to disaster recovery professionals. Good writing and great coverage probably explain why this title appears most often in college courses (both undergraduate and graduate offerings) that address disaster recovery planning as an entire or partial focus. Also a good reference for IT professionals involved in or tasked with DRP.

Disaster Recovery Testing: Exercising Your Contingency Plan (2007 Edition), by Philip Jan Rothstein (editor), Rothstein Associates, September 24, 2007, ISBN: 1931332422. The only title currently available that's devoted to the regular checklists, walkthroughs, and complete tests that DRP experts uniformly recommend should be conducted on a regular basis, to make sure that plans are workable, that participants know and can play their parts, and that the relationship between what the plan covers and what's going on in the business or enterprise remains current and correct.

Go.Recover-Data Center: *Data Center Disaster Recovery Plan on CD-ROM*, by Persson Associates, Rothstein Associates, June 4, 2002, ISBN: 1931332142. A collection of predefined worksheets in Microsoft Word format designed to make it easy for data centers to design and build reasonably comprehensive disaster recovery plans. This collection of templates is organized into a logical sequence of well-defined planning and documentation activities, all supported by 10 short supporting chapters on plan development.

High Availability And Disaster Recovery: Concepts, Design, Implementation: by Klaus Schmidt, Springer, July 11, 2006, ISBN: 3540244603. Combines a simple, straightforward, table-driven mathematical approach to availability and reliability that readers should find useful, along with helpful content on networking and data center considerations relevant to the central topics of high availability and disaster recovery.

Security Planning and Disaster Recovery, by Eric Maiwald and William Sieglin, McGraw-Hill Osborne Media, May 28, 2002, ISBN: 0072224630. Though this book doesn't include specific guidelines to or a template for building a disaster recovery plan (DRP) it does cover the subject matter reasonably well. That said, it does take a dual path approach to planning for information security as well as disaster recovery and will thus probably work best for those who must undertake both security and disaster recovery planning at the same time. This item should combine well with the Go.Recover Data Center offering, however.

The Backup Book: Disaster Recovery from Desktop to Data Center, 3e, by Dorian Cougias, et al, Schaser-Vartan books, July 1, 2003, ISBN: 0972903909. This book presents a very broad and therefore also fairly shallow coverage of the entire spectrum of disaster recovery topics (including but by no means limited to backups of many kinds). That makes this a good introduction to this subject matter but certainly not a be-all and end-all reference work. Best approached as a wayfinding tool on the subject of disaster recovery and prevention.

The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets, by Michael Wallace and Lawrence Webber, AMACOM, July 2004, ISBN: 0814472400. Those who recognize AMACOM as the publishing arm of the American Management Association (AMA) will already have said "Aha!" to this listing. Though not organized around a specific plan template, it does follow through the steps involved in building one and addresses important whys and wherefores at each point along that path.