UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Presented to the Interdisciplinary Studies Program:
Applied Information Management and the Graduate School of the University of Oregon
in partial fulfillment of the requirement for the degree of Master of Science

Key Stages of Disaster Recovery Planning for Time-critical Business Information Technology Systems

CAPSTONE REPORT

Travis S. Luckey
Director of Information Technology
VTM Group

University of Oregon
Applied Information Management
Program

February 2009

Continuing Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Linda F. Ettinger
Academic Director, AIM Program

Running Head: KEY STAGES OF IT DR PLANNING

Key Stages of Disaster Recovery Planning for Time-critical Business Information Technology Systems

Travis S. Luckey

VTM Group

Abstract

When disasters interrupt services provided by vital information technology (IT) systems, many businesses never recover (Decker, 2005). This review of literature published between 2001 and 2008 identifies key stages for consideration when performing IT disaster recovery (DR) planning to ensure business viability if disasters occur. Planning stages, presented as a guide for IT professionals, include Project Initiation, Conducting a Business Impact Analysis, Developing a DR Plan, Testing a DR Plan, and Maintaining a DR Plan.

Table of Contents

List of Tables **7**

Introduction to the Literature Review **9**
- **Purpose** **9**
- **Problem** **10**
- **Significance** **12**
- **Audience** **13**
- **Research Limitations** **14**
  - Topic focus. 14
  - Level of detail. 15
  - Intended audience. 15
  - Time frame. 16
  - Search strategy. 16
  - Literature collection and selection criteria. 17
  - The notion of “key elements.” 18
  - The notion of “best practices.” 18
- **Data Analysis Plan Preview** **18**
- **Writing Plan Preview** **19**

Definitions **21**

Research Parameters **27**
- **Research Questions and Sub-questions** **27**
- **Search Strategy** **28**
  - Selected databases and search engines. 29
  - Assessment of most productive databases. 30
  - Assessment of available literature. 32
  - Assessment of comparable literature reviews. 32
- **Evaluation Criteria** **33**
- **Documentation Approach** **35**
- **Data Analysis Plan** **36**
- **Writing Plan** **37**

Annotated Bibliography **41**

Review of the Literature **57**
- **Stage 1: Project Initiation** **57**
  - Securing management support 58
  - Organizing the planning project team 58
  - Establishing the project management process 59
  - Obtaining the required resources 60
  - Developing initial project objectives 61
- **Stage 2: Conducting a Business Impact Analysis** **63**

Gathering information 63
Identifying the time-critical IT systems 64
Performing a risk assessment 65
Prioritizing the recovery efforts 66
Stage 3: Developing a DR Plan 67
Selecting the risk management strategies 68
Defining disaster severity levels 68
Identifying activation triggers 69
Defining and documenting specific recovery processes 70
Selecting disaster response team members 72
Stage 4: Testing a DR Plan 73
Developing a test strategy 74
Training the recovery staff 74
Conducting the test procedures 75
Establishing the test frequency 76
Stage 5: Maintaining a DR Plan 77
Identifying potential sources of change 77
Selecting the change management strategy 78
Maintaining the planning documentation 79

Conclusions 81
Importance of Disaster Recovery Planning 82
Disaster Recovery Planning Stages 83
Achieving Comprehensive Disaster Preparedness 85

References 89

List of Tables

Table 1: Research questions and related DR planning themes 28

Table 2: Terms included with primary keywords to limit search results..... 29

Table 3: Notes on preliminary search experience..... 32

Table 4: Example objectives that can be specified within a DR plan 62

Table 5: Example prioritization of risks that face time-critical IT systems..... 66

Table 6: Alternatives for offsite system recovery..... 72

Table 7: Test methodologies that can be used to validate a DR plan..... 76

Table 8: Potential sources of change that can affect a DR plan 78

Table 9: Summary of the five DR planning stages..... 85

Introduction to the Literature Review

Purpose

Businesses are becoming increasingly reliant on information technology (IT) to improve operations and provide competitive advantage (Bhatt & Grover, 2005, p. 255). While the benefits of integrating IT into business operations are reportedly significant, the consolidation of important operations into information systems creates a serious liability since "most businesses could not continue to operate successfully if their IT services were unavailable" (Bradbury, 2008, p. 14). The primary risk, according to Decker (2005), is that the potential failure of IT infrastructure on which time-critical processes rely can increase the likelihood that companies will go out of business when disaster strikes (p. 44). Disasters, Decker (2005) explains, are business disruptions that result from "terrorist attacks, power outages, security breaches, nature and human error" (p. 44).

The purpose of this literature review is to describe key elements, supported by best practices, in disaster recovery planning for business information technology. In accomplishing this task, the study answers the following research question: "What are the most important elements of an effective disaster recovery plan for information technology systems?" In addressing the research question, this study will help companies to develop effective disaster recovery (DR) plans that are characterized by being clear and concise, focusing on the recovery of time-critical IT systems, and including strategies to test and revise the plans on a regular basis (Bradbury, 2008, p. 14). The key elements identified within this study are first categorized as themes during data analysis and then organized into stages that businesses can perform sequentially to guarantee fast and effective recovery after a disaster.

The notion of a 'key element' in this study is one that refers to a primary activity involved in developing, testing, or maintaining a disaster recovery plan, without which a disaster recovery effort would become "either ineffective or quickly outdated" (De Tura et al., 2004, p. 147). The identified elements are derived from recommendations made by professionals or academics in the field of disaster recovery planning and from case studies that examine disaster recovery methods employed by organizations. Case studies are a valuable resource for developing best practices since they can provide detailed analyses of disaster recovery scenarios and indicate specific techniques that have proven to be effective (*Case study*, n.d.).

Problem

IT disaster recovery is most often associated with a larger management process called "business continuity" planning (Alonso et al., 2001, p. 60). Business continuity (BC) management encompasses all of the strategic factors that must be addressed for a business to resume operations after a disaster occurs, including the availability of IT systems, personnel, facilities, and financing (Weiner, 2001, p. 25). As Clas (2008) warns, "today's customers want resilient suppliers" whose products and services are available at all times and as a result, even short periods of inaccessibility can "hinder a company's survival" (p. 45). Furthermore, in an economy where private companies provide an estimated 85 percent of the critical infrastructure, inadequate planning in the private sector can dramatically slow the recovery of communities after a major disaster takes place (Clas, 2008, p. 45).

Implementing a BC plan, explains Decker (2005), is "the only way" that an organization can "minimize the effects of disasters" (p. 44). Assessing the resources and processes on which a business depends and developing a plan to ensure operational integrity has more of an effect on

long-term viability than a company's reaction once a disaster occurs (Decker, 2005, p. 44). However, a comprehensive BC plan need not be completed in its entirety to improve a company's disaster preparedness. The development of a DR plan that focuses on recovering key business technology, explains Snedaker (2007), can still serve to protect an organization from a wide range of potential disasters (p. 4).

Acknowledging the importance of disaster preparedness, on August 3rd, 2007, former president George W. Bush signed the "Implementing Recommendations of the 9/11 Commission Act of 2007" into law (Clas, 2008, p. 45). Title IX of the act defined a new voluntary business preparedness certification program intended to "provide a method for businesses to assess their level of emergency preparedness" and to recognize the "potential benefits of being prepared" for disasters (Clas, 2008, p. 45).

The business preparedness certification program points to some existing BC planning standards developed for US government institutions and many of the program's details are still being defined (Clas, 2008, p. 45). Consequently, private companies that attempt to obtain the certification must make "progressive changes" to account for the needs of their unique environments (Clas, 2008, p. 46). Guidance for the required changes that relate specifically to the IT disaster recovery segment of a BC plan can be sought from sources such as the Information Technology Infrastructure Library (ITIL) (Tainter, 2008), which provides IT services management guidelines developed by the British government (*What is ITIL*, n.d.). However, Toigo (2003) notes that there are many alternative methodologies for recovering IT systems, which renders the process of developing DR plans for time-critical technology difficult and typically requires extensive trial and error (p. 30).

Without the guidance of a clear standard, the cost and complexity of preparing for disasters, combined with the misconception that a disaster won't take place, prevents many companies from undertaking planning activities (Weiner, 2001, p. 23) such as the development of an explicit strategy to recover time-critical IT systems. Moreover, among the organizations that do have BC plans in place, most are in the form of partial DR plans that "focus narrowly on the backing up of basic data rather than broadly on preventing the losses that accompany a major disaster" (Weiner, 2001, p. 23).

Significance

Disasters interrupt operations for over 90 percent of businesses, nearly half of which close their doors within five years (Decker, 2005, p. 44). Furthermore, 60 percent of North American businesses do not have an adequate plan in place to resume vital IT services after a disaster (Chisholm, 2008, p. 11). The lack of planning is due to several assumptions common among business executives. These assumptions are that (a) a disaster won't occur, (b) the business could survive a major IT failure, or (c) insurance coverage would provide adequate protection (Teuten, 2005, p. 45). Teuten (2005) explains that these assumptions are the top three mistakes that companies can make when attempting to manage risks such as disasters (p. 45).

To address this liability, Hayes (2005) suggests that businesses create disaster recovery (DR) plans for IT systems that the businesses determine are essential to operations (p. 29). A DR plan is defined as one that "details the key activities required to reinstate IT services within agreed recovery objectives" after business operations have been interrupted by a disaster (Bradbury, 2008, p. 15). Snedaker (2007) expands upon this definition, explaining that disaster

recovery involves the actions necessary to quickly stop a disaster's effects as well as to address the immediate aftermath (p. 4).

Although every business should develop a DR plan, warns Lesser (2005), the high level of complexity and tight budgets inherent to business IT environments present several challenges (p. 70). The challenges to DR planning include: (a) ensuring that a recovery plan will work as intended, (b) determining when a plan should be activated, and (c) documenting "that best efforts have been made to protect the business from a full range of potentially disruptive eventualities" (Lesser, 2004, p. 70).

Audience

The target audience selected for this literature review is primarily IT professionals who are tasked with implementing or improving a DR plan. As noted by Ryan & Ryan (2005), ensuring that vital IT services are available when needed is a core principle within the information security branch of information management (p. 141). As a result, the goals involved in DR planning are closely tied to the goals in the larger area of information security. In addition to ensuring IT system availability, information security personnel are responsible for preventing corruption of and controlling access to all the information stored by an organization (Ryan & Ryan, 2005, p. 141).

This literature review is designed to aid IT professionals as they collaborate with business managers to determine (a) how each functional area depends on IT, (b) which IT systems are time-critical, and (c) how to recover those systems after a disaster. And, by highlighting the potential impacts of disasters on key IT systems and supporting the assertions with credible

sources, the literature review may also help IT professionals to gain executive support for DR spending, which, according to Cerni (2006), often poses a challenge to DR planning.

Chernicoff (2007) explains that the IT professionals tasked with DR planning often work on a team that includes empowered decision-makers such as department heads who are tasked with overseeing the development of the DR plan or a larger BC plan (p.49). Understanding DR factors at a high level can help such team members to prioritize technological considerations along with other factors relevant to the planning initiative (Cerni, 2006). Therefore, the individuals responsible for overseeing the development of a DR plan or a comprehensive BC plan constitute a secondary audience for this literature review.

The outcome of this study is structured as a guide that is based on information derived from real-world case studies along with advice from experts in the DR planning field. The guide identifies major themes, presented as sequential stages, that the selected literature indicates are essential to the development of a DR plan. The guide further describes the key elements within each theme that should be considered by the individuals who are developing DR plans, such as a risk assessment and a change management strategy (Cerni, 2006). Elements are supported by best practices also identified in the selected literature. In this context, “best practices” refers to “methods and techniques that have consistently shown results superior than those achieved with other means, and which are used as benchmarks” for which to strive (*Best practice*, n.d., para. 1).

Research Limitations

Topic focus. Disaster recovery planning for information technology systems is linked to the larger topics of information security (Ryan & Ryan, 2005, p. 141) and business continuity planning (Alonso et al., 2001, p. 60). The discussion of information security within this literature

review is limited to establishing the connection between DR and the broad subject of information management, and describing the professional responsibilities associated with the IT security personnel who typically develop DR plans.

Business continuity plays a much more significant role than information security within this literature review since DR is described as “the core” principle of BC planning (Drummond, 2008, p. 14), and in some cases the two phrases are used interchangeably (Spencer & Johnston, 2003, p. 89). As a result, literature associated with BC planning plays a central role in this review. However, the use of BC literature is generally limited to instances in which such resources discuss (a) the principles of DR planning, (b) how DR relates to a larger context, or (c) external factors that affect DR planning such as budget allocation for a plan’s development.

Level of detail. The selected literature indicates that businesses depend on a wide variety of complex IT systems. Specific disaster recovery procedures for each time-critical IT system should be developed by a team with expertise in that specific business and technical environment (Chernicoff, 2007, p. 49). Consequently, this best practices guide will not describe granular recovery procedures for specific technologies. Rather, it will provide an overview of relevant considerations to guide such a team as they develop, test, and maintain a DR plan.

Intended audience. This literature review is designed to serve as a guide that describes key elements to be considered by those tasked with developing a DR plan in a professional environment, typically IT professionals and a management team (Chernicoff, 2007, p. 49). The audience should be familiar with the requirements for a specific technical infrastructure and business environment in order to adequately determine how this guide’s principles should be

applied. This study is not intended to benefit other audiences such as business professionals that may be affected by a DR plan but are not directly involved with its development.

Time frame. Although "the need for disaster recovery has always existed," the September 11, 2001 attack on the World Trade Center increased awareness and invoked revision to existing DR planning approaches (Jrad et al., 2004, p. 107). An analysis of preliminary search results indicates that it is difficult to distinguish the specific key elements and related best practices rendered obsolete by these changes. In order to reduce the likelihood of obsolete information becoming a part of this guide, sources published prior to September 2001 are not used in this literature review.

Search strategy. The search for the elements of a disaster recovery plan is limited to those that are relevant to information technology systems in business environments. Due to the association between the two subjects, searches for sources relevant to IT disaster recovery include literature that addresses business continuity planning. However, BC planning covers a number of other related subjects (Clas, 2008, p. 46), most of which are excluded from this literature review. The excluded subjects address BC planning concerns in the following areas: (a) protection of facilities and assets, (b) availability of financial resources, (c) accessibility of personnel, and (d) non-IT operations such as manufacturing (Clas, 2008, p. 46).

Similarly, searches for DR within the larger subject of information security exclude unrelated information security concerns such as the confidentiality and integrity of data stored electronically by a business (Ryan & Ryan, 2005, p. 141). However, many sources that address relevant DR principles also include a discussion of excluded topics. As a result, inapplicable BC

and information security topics are not automatically excluded from search results using keywords or special operators, but are subjected to secondary review.

Literature collection and selection criteria. Resources that provide the literature for this review include online scholarly indices and the University of Oregon (UO) Portland library. Online indices are parsed using a set of keywords that include “disaster recovery” or related subjects. The indices used are considered to be scholarly due to the presentation of sources that are peer-reviewed or feature bibliographic information within the first two pages of the search results. General World Wide Web search engines such as Google and Yahoo are excluded due to a lack of prominently noted scholarly sources.

Preferred sources selected for this literature review address topics directly relevant to DR planning for IT systems. Additional sources are used to establish the framework for this review, such as those that associate DR planning with other information management subjects or provide key-term definitions.

Preferred sources are selected using specific criteria to certify credibility. Sources judged to be scholarly rather than popular are preferred since, according to Smith (2006), “most academic work will favor scholarly sources” over those that are popular (para. 1). Sources are evaluated across the following set of desirable criteria: (a) authors should have become experts in their field through research or experience, (b) sources should provide citations or a bibliography, (c) sources should have been subjected to a peer-review process, and/or (d) publishers should be scholarly or professional organizations (Smith, 2006).

It is not necessary for sources to meet all of these criteria in order to be judged credible. For example, Smith (2006) notes that an article published in a trade magazine may not include

citations or be subjected to a peer-review. However, such a source would be deemed credible if it provides explicit background information to indicate that the author is an experienced professional in the field of IT disaster recovery planning.

The notion of "key elements." The selected literature discusses numerous activities that play a role in DR planning. While the specific focus and terminology varies between each resource, authors tend to agree on several primary activities that should be performed as a part of any DR planning initiative (Bradbury, 2008, p. 16). Within this document, key elements are limited to those activities that are vital to the development, testing, or maintenance of a disaster recovery plan. Elements are evaluated to be vital if a disaster recovery effort would become "either ineffective or quickly outdated" without them (De Tura et al., 2004, p. 147). DR planning activities that the literature indicates to be applicable only in rare cases are excluded.

The notion of "best practices." Although this study presents strategies for navigating elements of a DR plan based on approaches found to be effective by other organizations, the best practices identified are not necessarily applicable in every situation (*Best practice*, n.d.). Furthermore, this literature review takes the position that it is possible for multiple approaches to be equally valid when addressing a single issue (Leedy & Ormrod, 2005, p. 133). It is ultimately the readers' responsibility to identify how their unique environments should interpret and apply the best practices identified in this literature review.

Data Analysis Plan Preview

This inquiry is structured as a review of literature that "evaluates, organizes, and synthesizes" existing knowledge (Leedy & Ormrod, 2005, p. 77) in order to develop a new perspective (Obenzinger, 2005, p. 1). The new perspective is expressed in the form of a guide

that identifies the key elements to effective DR planning. Doing so requires the analysis of a large body of selected literature to reveal specific “methods and techniques that have consistently” shown superior results to alternative approaches (*Best practice*, n.d., para. 1). Literature is obtained using keyword searches and carefully evaluated to gauge both relevancy and credibility. Sources meeting those requirements are compared to identify commonalities among DR planning approaches that have been proven by others to be effective.

Resources that satisfy the evaluation criteria are interpreted using a qualitative research approach known as conceptual analysis (Busch et al., 2005). This approach places a strong emphasis on unraveling complex issues (Leedy & Ormrod, 2005, p. 133), such as those that surround DR planning activities in real-world environments. As noted by Busch et al. (2005), when conducting a conceptual analysis a researcher first identifies research questions and then codes them into manageable content categories. The coding process allows the researcher to focus specifically on “words or patterns that are indicative of the research question” (Busch et al., 2005, para. 1).

Writing Plan Preview

In order to identify the key elements and related best practices for DR planning, this study examines a variety of scholarly sources. The objective in doing so is to seek out and present the common themes between sources that have proven effective in real-world environments. Presentation of the information follows the “thematic” pattern of organization, in which the literature review closely examines current DR practices rather than providing a history of the topic to illustrate how it may have changed over time (*Literature review*, 2007, para. 27).

Typical of the thematic approach, a section is dedicated to each of the major common themes, or subtopics, identified during the data analysis phase among selected DR planning resources (*Literature review*, 2007). These sections are combined to form a guide, designed for IT professionals and managers tasked with implementing or improving a DR plan, which (a) describes key elements and effective methods, (b) suggests resources that may be useful, and (c) warns about potential problems of which DR planners should be aware. The DR planning themes addressed in this guide are compiled from information provided by the following authors: Bradbury (2008), Chisholm (2008), Clas (2008), Gondek (2002), Gregory (2008), Rothstein (2007), Snedaker (2007), Spencer & Johnston (2003), Toigo (2003), and Wells et al. (2007). Themes include Project Initiation, Conducting a Business Impact Analysis, Developing a DR Plan, Testing a DR Plan, and Maintaining a DR Plan.

Definitions

Specialized terminology used within this literature review is drawn from the selected literature as well as academic sources and reference materials. These terms include technical terminology, such as jargon that is characteristic of the disaster recovery planning field (*Jargon*, n.d.), as well as business and academic phrases that describe structural components of the literature review. Although some of these terms are defined in-text at the point at which they are introduced, many are withheld to prevent interruptions to the flow of the document. This section provides definitions to ensure that the contextual meaning of all words and phrases used within this study are clear to the audience.

Best practices – The "methods and techniques that have consistently shown results" that are superior to "those achieved with other means, and which are used as benchmarks to strive for." (*Best practice*, n.d., para. 1). What works best for one organization may not be ideal for others, however, "and no best practice remains best for very long as people keep on finding better ways of doing things" (*Best practice*, n.d., para. 1).

Business Continuity (BC) planning – The process of identifying all of the factors that must be addressed for a business to resume operations after a disaster occurs, including the availability of IT systems, personnel, facilities, and financing (Clas, 2008, p. 46).

Business Impact Analysis (BIA) – A study of an organization's IT systems that aims to determine which resources warrant the expense and effort of distinct inclusion in a disaster recovery plan (Gregory, 2008, p. 51). A BIA further specifies the priority by which each time-critical system is recovered after a disaster (Bradbury, 2008, p. 16).

Case study – A "documented study of a specific real-life situation or imagined scenario" that is "used as a training tool in business schools and firms" (*Case study*, n.d., para. 1). Observers then "analyze the prescribed cases and present their interpretations or solutions, supported by the line of reasoning employed and assumptions made" (*Case study*, n.d., para. 1).

Cold backup site – A leased building space that is largely empty but can be used to setup temporary equipment to replace damaged IT systems (Wells et al., 2007, p. 146).

Competitive advantage – The positioning of a firm in its industry to "raise entry barriers, increase bargaining power with suppliers and customers, offer new products and services, or change the rules of competition" (Bhatt & Grover, 2005, p. 255).

Critical infrastructure – The systems and services on which communities rely to provide "power, water, transportation, communication, and food" (Clas, 2008, p. 45).

Cutover tests – A DR plan test methodology in which time-critical IT systems are temporarily replaced by backup systems that are developed by following the steps outlined in a DR plan (Gregory, 2008, p. 231).

Disaster – A disruption that results from "terrorist attacks, power outages, security breaches, nature and human error" (Decker, 2005, p. 44). The defining characteristics of disasters include suddenness, unexpectedness, and significant destruction and/or adverse consequences (*Guide for developing a disaster plan*, 2006).

Disaster Recovery (DR) planning – The process of developing an explicit strategy that "details the key activities required to reinstate IT services within agreed recovery objectives" after business operations have been interrupted by a disaster (Bradbury, 2008, p. 15).

Electronic data – Information in a digital form that has been manipulated by computer software (*Data*, 2003).

Hardware – Physical assets that make up a computer system such as network servers and storage devices (*Hardware*, n.d.).

Hot backup site – A facility that is fully equipped to assume the responsibilities from damaged IT systems with little or no preparation (Gregory, 2008, p. 147).

Information availability – The extent to which the requestor of a specific set of electronic data receives the requested data in an acceptable time interval (Ryan & Ryan, 2005, p. 142).

Information management – The broad field of study that deals with the collection, interpretation, and storage of data from sources inside and outside an organization for the purposes of threat protection, use monitoring, value quantification, business forecasting, and legal compliance (North et al., 2004, p. 172).

Information security – "The discipline responsible for protecting valuable information assets and systems," which are "characterized by requirements for (a) privacy or confidentiality, (b) assured integrity through the prevention of illicit modification or destruction, and (c) ready availability" (Ryan & Ryan, 2005, p. 141).

Information Technology (IT) – The electronic systems on which businesses depend for the "storage, summary, and transmission" of information (North et al., 2004, p. 167).

Key element – A primary activity involved in the development, testing, or maintenance of a disaster recovery plan, without which a disaster recovery effort would become "either ineffective or quickly outdated" (De Tura et al., 2004, p. 147).

Keywords – A set of words or phrases selected to describe a desired subject for the purpose of seeking out related articles that take "into account the semantic and linguistic extensions of the search context" (Caramia & Felici, 2006, p. 2771).

Maximum Tolerable Downtime (MTD) – The maximum length of time that a critical IT system can be unavailable before a business fails (Gregory, 2008, p. 72).

Paper tests – A DR plan test methodology that involves the review and revision of DR documentation by independent members of the response team (Gregory, 2008, p. 221).

Parallel tests – A DR plan test methodology in which members of the disaster response team perform the activities prescribed to them by the DR plan as if a disaster had occurred (Gregory, 2008, p. 227). However, these tests stop short of interrupting the services provided by the business' time-critical IT systems (Gregory, 2008, p. 228).

Peer-review – An evaluation of the quality of work performed by "a member of a peer group by the experts drawn from that group" (*Peer review*, n.d., para. 1). As it applies to this literature review, peer-reviewed articles are those in which colleagues have assessed "the value of a contribution to the field by determining if a research report is publishable in the group's journal" (*Peer review*, n.d., para. 1).

Portable Document Format (PDF) – An electronic file format developed by Adobe Systems that "captures formatting information from a variety of desktop publishing applications" and requires the Adobe Reader application in order to be viewed (*PDF*, n.d., para. 1).

Reciprocal agreements – An accord between two organizations to host each other's backup hardware that can be activated in the event of a disaster (Wells et al., 2007, p. 147).

Recovery Point Objective (RPO) – The amount or extent of data loss that a business can tolerate from a time-critical business IT system that was damaged by a disaster (Snedaker, 2007, p. 219).

Recovery Time Objective (RTO) – The time period in which an organization must have an IT system restored to operation after a disaster has taken place (Gregory, 2008, p. 72). The RTO is always less than the MTD to allow for work recovery (Snedaker, 2007, p. 219).

Risk management – The activities performed to identify and prepare for "events or surroundings that can adversely affect the organization and its resources (e.g., people, facilities, technologies) due to business interruption, the potential loss such events can cause, and the controls needed to avoid or mitigate those outcomes" (Clas, 2008, p. 47).

Risk mitigation – Taking steps to systematically reduce the adverse effects of an event such as a disaster (*Risk mitigation*, n.d.). These steps can include making modifications to an environment to avoid or reduce the impact of a potential risk (Snedaker, 2007, p. 265).

Simulation tests – A DR plan test methodology that attempts to duplicate entire network environments, to the extent possible, in a controlled laboratory environment (Lesser, 2004, p. 70).

Time-critical systems – The technology on which key business processes rely and that must be "specifically prioritized" for prompt recovery after a disaster occurs (Conz, 2008, p. 32).

Vendor-supplied agreements – An accord in which a vendor is designated to provide and host replacement IT systems for a business to use after a disaster (Wells et al., 2007, p. 149).

Walkthrough tests – Also called "talk through" tests, walkthrough tests are a DR plan test methodology that requires response team members representing each business unit to

meet and describe the procedures that would be followed after a disaster takes place (Gondek, 2002, p. 17).

Warm backup site – A leased building space in which organizations store replacement hardware (Gregory, 2008, p. 148). The hardware is not configured, however, so software installation and data restoration must be performed in order for the site to assume the responsibilities of damaged IT systems (Gregory, 2008, p. 148).

Research Parameters

This section explains the structured approach that is employed to frame the research design of this study. Based on the results from exploratory research, a strategy is established to guide continued searches and describe the criteria that are used to evaluate information sources. A method is defined by which resources deemed credible and relevant to the information search are documented. Processes are then characterized by which pertinent data is mined and presented from documented resources.

Research Questions and Sub-questions

This research effort is guided by a series of research questions. The questions are each designed to investigate DR planning themes that, when answered collectively, will sufficiently address the overarching research question: "What are the most important elements of an effective disaster recovery plan for information technology systems?" Table 1 (see below) illustrates these guiding questions and sub-questions, and indicates which of the DR planning themes is addressed by each question.

Research questions & sub-questions	Related DR planning theme
1. What constitutes a "disaster" in the context of DR planning for business IT systems? **a. Does the concept of a disaster vary depending on the size, structure, or purpose of an organization?** **b. Should companies define multiple types or severities of disasters and develop different plans for each?**	Project Initiation
2. What are the requirements to effectively begin a DR planning initiative? **a. What departments within an organization should be involved?**	Project Initiation

Research questions & sub-questions	Related DR planning theme
b. How should resources be obtained?	
3. How should companies determine the time-critical IT systems that should be covered by a DR plan?	Business Impact Analysis
4. How should the recovery of time-critical systems be prioritized?	Business Impact Analysis
5. How should companies define the recovery process and the flow of activities for each time-critical system?	Developing a DR Plan
6. What should companies do to control, plan, distribute, and account for the costs of DR planning?	Developing a DR Plan
7. What are the best practices for testing a DR plan? **a. How often should a DR plan be tested?** **b. What characterizes a sufficient test?**	Testing a DR Plan
8. How should a DR plan be reviewed to determine if updates are necessary? **a. What types of events should trigger updates?** **b. Who should be involved in the reviewing and updating process?** **c. How should revisions to DR planning documents be controlled?**	Maintaining a DR Plan

Table 1: Research questions and related DR planning themes

Search Strategy

Although the focus of this literature review is IT disaster recovery planning, considerations relevant to the subject are often discussed within the larger context of business continuity planning (Alonso et al., 2001, p. 60). Exploratory keyword searches reveal that articles on business continuity do not necessarily include the keywords “disaster recovery.” In order to capture relevant information in such sources, searches for literature use both “disaster recovery” and “business continuity” as primary keywords.

Initial searches for “disaster recovery” or “business continuity” produced hundreds of results regardless of the index used. Some results indicate that disaster recovery is an established term that deals specifically with IT infrastructure in business environments (Bradbury, 2008, p. 15). However, there are many other results that deal with unrelated topics. For example, some results for “disaster recovery” include the effects of natural disasters on agriculture, while some results for “business continuity” do not discuss technological considerations.

The search strategy based on these initial findings is to combine the keywords with additional terms such as “technology” or “business” to limit the results. Words for which multiple suffixes could be valid, such as “technology” and “technologies,” are submitted with asterisk characters (*) to allow all ending variations to be returned. After much experimentation, the terms illustrated in Table 2 (see below) are determined to be the most effective at reducing extraneous results from those that address DR planning for time-critical IT systems:

Search terms combined with “disaster recovery” (most effective listed first)	**Search terms combined with “business continuity” (most effective listed first)**
1. technolog*	1. technolog*
2. business	2. information manage*
3. information system*	3. information security
4. information security	4. principle*
5. information manage*	5. plan*
6. business continuity	6. information availability
7. plan*	
8. information availability	

Table 2: Terms included with primary keywords to limit search results

Selected databases and search engines. Through trial and error and with the advice of a professional reference librarian, six online indices are determined to be the most ideal because they include many sources that focus on business or technology. Listed in descending order and beginning with the index that produced the most relevant results, the selected indices are: (a)

Business Source Premier, (b) ArticleFirst, (c) Lexis-Nexis Academic, (d) Academic Search Premier, (e) Google Scholar, and (f) INSPEC.

Assessment of most productive databases. Each of the selected databases produced at least some "good" results. In the context of this inquiry, good results are defined as those that describe factors relevant to DR plans for business IT systems or the larger context of BC management. Those factors of most interest aligned with one of three sub-areas: (a) components that make up a DR plan; (b) information about why DR plans are effective or ineffective; and (c) suggestions for how to implement, test, and maintain a DR plan.

Other criteria used to judge good results are: (a) must include full-text and be published in a peer-reviewed journal; (b) must be written by an expert or the faculty of an accredited university; or (c) must be a published textbook that addresses the areas of risk management, BC planning, or DR for IT systems within business environments. Sources are also limited in time to those written after September 11, 2001. The terrorist attacks on the World Trade Center raised awareness about the need for risk management planning, which led many businesses to revise existing DR planning processes (Jrad et al., 2004, p. 107).

Due to the technical nature of the DR topic, perspective is supplemented with articles from trade publications. However, a subject matter expert is less likely to have reviewed articles in these sources prior to publication, so it is more difficult to evaluate accuracy (Smith, 2006). Only contributions to such articles made by experts in the field of information security or business continuity planning are considered to be reliable. Other content obtained from trade publications is limited to ideas for consideration rather than statements of fact.

A summary of the preliminary search experience through each of the six selected indices is provided in Table 3 (see below). Within each index, various combinations of the selected keywords are used and the quantity of good results is recorded. The overall time spent with each index is also tracked, along with notes to detail the individual search processes. Indices with the highest ratio of good results relative to the time spent searching are the most beneficial to this literature review. For that reason, the table is organized to list indices starting with the highest ratio and descending to the lowest.

Online index	**Time spent searching**	**"Good" results**	**Search notes**
Business Source Premier	10.5 hours	29	Many of the good resources are presented on the first page of results. The good results taper off quickly regardless of the search terms used, so keyword effectiveness can be gauged quickly. Most valuable keyword combination is "disaster recovery AND technolog*," with results limited to peer-reviewed journal articles.
ArticleFirst	4.5 hours	12	This index provides relevant results that do not overlap with other indices. However, searches are often delayed because all ports are in use. "Disaster recovery AND technolog*" was again the most effective keyword combination.
Lexis-Nexis Academic	5.0 hours	11	This index produces hundreds of articles regardless of keyword combination. Many undesirable resources clutter the results and increase the time needed to find valuable articles. The problem stems from the broad array of subjects included in this index. Including the keywords "business" or "technolog*" is helpful in reducing results from other subjects such as healthcare.
Academic Search Premier	3.0 hours	5	Many of the results produced by this resource overlap with the Business Source Premier index. This index also has a high percentage of results on unrelated topics such as the effects of drought on farming. This index is only used when searches elsewhere prove

Online index	Time spent searching	"Good" results	Search notes
			fruitless. Searches on this index require the use of multiple keywords connected with multiple AND statements to reduce undesirable results.
Google Scholar	4.0 hours	6	Google Scholar is determined to be the best index to find resources that establish the connection between IT DR, information availability, information security, and information management. Google Scholar produces results that support this endeavor from trade publications and academic websites.
INSPEC	1.5 hours	2	This resource provides many results with relevant abstracts that are not included in other indices. However, it does not produce many sources for which full text is available. INSPEC is primarily used with the expectation that sources found need to be ordered from the UO library.

Table 3: Notes on preliminary search experience

Assessment of available literature. Preliminary searching produced over 60 credible references that could have proven valuable to this study. Further examination revealed that some of the information sources described unusual cases or provided information that was too broad to be useful. Additional searches through online and library resources have produced a revised list of over 40 valuable resources that include textbooks, Web pages, and articles published in peer-reviewed journals and trade publications.

Assessment of comparable literature reviews. Searches for variations of "disaster recovery" and "literature review" on Academic Search Premier, Business Source Premier, and ERIC did not produce any comparable reviews of literature. While the search was not exhaustive, the results indicate that this may be one of the first literature reviews to be published that directly addresses the subject of DR planning for time-critical IT systems.

Evaluation Criteria

In order to develop a guide that can be used for DR planning by businesses in a variety of industries, the literature selected for this review is drawn from a wide array of sources. Although some information is accessed through the UO Portland library, literature is primarily collected using keyword searches from online indices that distribute articles addressing many business and technical disciplines. The database from which the majority of sources are drawn, Business Source Premier, produces full text articles from over 8,800 publications that address business, management, economics, banking, finance, accounting, and technology topics (*OneSearch*, n.d.).

Prior to conducting a keyword search on each index, results are restricted to articles published on or after September, 2001. Doing so ensures the currency of the results, since the terrorist attacks of September 11, 2001 increased awareness and inspired revision to DR processes for business IT systems (Jrad et al., 2004, p. 107). Eliminating dated information is critical since this literature review is intended to convey the current best practices to its audience. Setting this limitation prior to conducting the search reduces the time needed to evaluate search results since the indices automatically withhold articles that are potentially obsolete.

After setting the date filter and conducting a keyword search, the results within each index are examined to identify whether or not the inclusion of information within the results will be valuable to those responsible for DR planning. Information considered to be relevant includes topics that relate to DR planning for business IT environments or to the larger subject of BC management. In response to keyword submissions, the indices generally present the titles of 20 results per page. Abstracts are read for the search results with titles indicating that the content

may be pertinent to the information search. In the event that no results with relevant titles are included in the first two pages of results, the keywords are revised and the search is repeated.

After identifying resources in which content is relevant to this study's audience, the credibility of each resource is evaluated to guarantee that the quality of the information contained within is sufficient for this academic literature review (Smith, 2006). Multiple factors are used to evaluate the credibility of resources with the objective of identifying scholarly sources wherein the content is appropriate (Smith, 2008). The authority of the author and the publisher are first inspected to certify that each is "qualified to speak to the topic(s)" (Smith, 2008, para. 3) of DR or BC planning. Preference is given to works written by academics or experts rather than popular sources whose authors, according to Smith (2006), may include journalists or freelance writers. Information attesting to the qualifications of the authors can be found at the beginning or the end of most of the resources selected for this literature review. Works published by scholarly, professional, or academic institutions are also chosen over those released by commercial or for-profit organizations.

Another factor used to gauge the credibility of sources is the inclusion of citations or a bibliography. The presence of these elements, explains Smith (2006), suggests that the information is valid and well researched. However, references to prior work are examined to determine if they are authoritative on the subject for which they are cited. Resources that do not cite recognizable authorities may still be credible when derived from a peer-reviewed source such as a journal. Peer-reviewed sources are those that have been evaluated by experts within the industry for which the source is targeted (*Peer review*, n.d.). Sources that have been subjected to

a peer review by an editorial board of outside experts are likely to be scholarly (Smith, 2006), and as a result, are deemed credible for this literature review.

Documentation Approach

Literature that is located using searches on the selected indices or at the UO library are coded by hand to determine whether or not they contain information relevant to this synthesis of DR planning best practices. Coding by hand is preferred to an automated method since preliminary research reveals that business continuity articles often refer only implicitly to DR concepts, a situation in which Bush et al. (2005) warns that automated coding tools are more error prone. When the coding process reveals that an article contains at least one instance of a relevant DR planning concept, the article is documented to facilitate retrieval and citation.

Documented resources are stored electronically along with information about the author, publisher, and other factors that establish credibility. Full-text articles are converted to the Adobe Portable Document Format (PDF) for storage. The following file naming convention is used for each resource: Author's Last Name_Year Published_ Subject. The subject within the file's name uses the abbreviations "DR" for "Disaster Recovery" and "BC" for "Business Continuity." This format allows articles cited in-text to be identified quickly when more information is needed.

While full-text articles that are obtained online are saved electronically, published abstracts, APA-formatted citations, and descriptive notes for each resource including textbooks are consolidated into a separate document. Abstracts are valuable for documentation because they present a document summary that can be quickly evaluated to interpret the gist of the subject matter (*Abstract*, n.d.). Whenever a published abstract is not available for a selected resource, a brief summary that includes relevant keywords, such as disaster recovery or business

continuity, is written. Resources that provide more depth than others are highlighted in green within this summary document so that they stand out as preferred resources. The separate document eases the location of information within selected sources and facilitates the rearrangement of resources to reveal logical progressions when writing (Obenzinger, 2005, p. 6).

Data Analysis Plan

Key elements and supporting best practices in DR planning presented in this literature review are derived from expert recommendations and case studies across a variety of industries. Information from a range of environments is synthesized to reveal methods and techniques that are widely applicable. Elements within case studies are identified first by seeking credible resources that describe DR scenarios, and then by evaluating the principles at work in each scenario (Heffes, 2002, p. 45). Doing so ensures that a relationship exists between the selected element defined and the desired result of an effective DR plan, as described in the supporting best practice (Heffes, 2002, p. 45). This process also makes it possible to determine whether the conclusions in the literature are "justified based on the data presented," which, according to Leedy & Ormrod (2005), is a key concern within literature reviews (p. 77).

Resources identified as both relevant and credible are interpreted using a conceptual analysis process. Busch et al. (2005) explains that a conceptual analysis is a process used to choose one or more concepts and determine whether or not said concepts are present within a selected set of sources. The conceptual analysis is used to determine that the selected works discuss the desired concepts in a relevant context (Busch et al., 2005).

To perform this conceptual analysis on DR planning, the coded phrases "disaster recovery" and "business continuity" must be present within the resource as well as at least one of

the following terms that research reveals are used most frequently when describing DR planning concepts: (a) technology, (b) IT, (c) computers, or (d) information systems. Selected works are coded for the existence rather than the frequency of these phrases, so that the concept of IT disaster recovery, for example, is only counted a single time within a selected resource (Busch et al., 2005). Furthermore, variations on the coded words such as "technologies" rather than "technology" are accepted so long as a review of the surrounding content indicates that the implied meaning is generally the same.

Initial searching indicates that often when the concept of "technology" is discussed along with "disaster recovery," IT DR topics are being described. However, it is possible that a piece of literature including both phrases could be describing unrelated topics such as air conditioning systems. To account for such a scenario, Busch et al. (2005) suggests that a translation rule by which concepts are interpreted is used when coding each resource. In this study, the translation rule specifies that only references to technology for which the context is interpreted as speaking about business IT systems be coded as valid instances. Since the purpose of the coding effort is to determine whether or not resources speak about concepts relevant to this literature review, information deemed irrelevant to the coding process is ignored (Busch et al., 2005).

Writing Plan

Information regarding DR planning key elements and best practices is first derived from resources that are deemed relevant to this review by the conceptual analysis process, described above in the *Data Analysis Plan* section. These key elements and supporting best practices are then synthesized into an organization that follows a thematic model, which examines common

threads among a variety of scholarly sources (*Literature review*, 2007) concerning DR planning for business IT systems.

When determining whether or not a coded concept can be assigned to the status of "key element", a comparison is made to the guiding definition provided by De Tura et al. (2004): A primary activity involved in the development, testing, or maintenance of a disaster recovery plan, without which a disaster recovery effort would become "either ineffective or quickly outdated" (p. 147). Additionally, since best practices are prone to change (*Best practices*, n.d.), the thematic model utilized in this review takes a "state of the art" approach that focuses on the current methods (Busch et al., 2005, para. 1) preferred by DR planners rather than the evolution of the subject over time (*Literature review*, 2007). Presenting a guide that is based on current information about key elements and proven methods will prevent the audience from having to devote "scarce resources to inventing new techniques" (Heffes, 2002, p. 44).

The synthesis of common threads within the literature on DR planning reveals several relevant themes. Following the thematic organizational model, each theme is discussed within this literature review in a dedicated subsection (*Literature review*, 2007). Although a reader seeking guidance on a specific DR planning area could move directly to the subsection in which the desired information is discussed, this document is not designed for the subsections to be interpreted independently. Concept definitions and background information are not repeated within each subsection. Attempting to skip subsections may create confusion or cause readers to overlook important planning elements. These problems could lead to the development of incomplete or ineffective DR plans.

A preliminary review of the selected literature reveals five themes as potentially most relevant to DR planning. This guide organizes the five themes sequentially, whereby the key elements derived during data analysis that are typically conducted at the beginning of a DR planning endeavor, are listed first. These elements are referred to as "activities" throughout the guide when actions are being described. Additional activities are introduced in the order that the literature identifies that each should be performed. The five preliminary DR planning themes anticipated within this guide, which are presented as stages, include:

1. **Project Initiation**: In this stage, the need for DR planning as a component of a BC management program is established and resources are obtained (Clas, 2008, p. 47). Initiation activities include establishing the potential business value of DR planning, organizing the project and planning team, identifying success criteria, and obtaining support from upper management (Snedaker, 2007, p. 54). In addition to providing the resources needed for planning activities, management can help a DR planning team to understand how business processes interrelate and how information flows through an organization (Wells et al., 2007, p. 33)
2. **Conducting a Business Impact Analysis (BIA)**: The next stage in DR planning is to conduct a business impact analysis that identifies the systems on which time-critical business processes rely and the recovery priorities (Bradbury, 2008, p. 16). In addition to subject matter experts and members of the management team, Barrier (2001) suggests that this process can seek input from internal auditors who understand how business processes interrelate (p. 57).
3. **Developing a DR Plan**: At this stage, Bradbury (2008) explains that companies must define the recovery process and the flow of activities for each of the time-critical systems

identified in the BIA (p. 16). These include the identification of prerequisites and dependencies for each activity (Bradbury, 2008, p. 16), the specification of who will perform specific recovery tasks, and the establishment of service-level agreements to guarantee the recovery of needed systems by external vendors and suppliers (Hlavacek et al., 2004, p. 179).

4. **Testing a DR Plan**: According to Chisholm (2008), during the testing stage businesses attempt to validate a DR plan to verify that it will work as intended (p. 11). Rothstein (2007) warns that without testing, DR planning activities are "an exercise in speculation" (p. ix). Several alternative testing methodologies are described that include conducting paper tests, walkthrough tests, simulations, parallel tests, and cutover tests (Gregory, 2008, p. 219).
5. **Maintaining a DR Plan**: The final stage identified in this DR planning guide describes activities and considerations that can guarantee that a DR plan remains useful as time passes. This includes making revisions to account for changes in business priorities, IT system architecture, and personnel (Gondek, 2002, p. 18). Toigo (2003) explains that needed changes can be signaled through change management procedures and testing (p. 427). De Tura et al. (2004) adds that the maintenance stage of DR plan development is iterative: earlier stages should be revisited and revised based on lessons learned from the execution of a disaster recovery plan (p. 158).

Annotated Bibliography

All references selected for use in this study are evaluated and prioritized, and only those that are judged to be the most significant to a synthesis of DR planning best practices are selected for presentation in this section of the document (Obenzinger, 2005, p. 4). This annotated bibliography, consisting of 21 entries, provides citations for the literature that comprise the core data set used for content analysis. The annotated bibliography supplements the listing of each selected reference with a summary of its content, an assessment of its credibility, and a reflection about its relevancy to this study (Stacks & Karper, 2008).

Alonso, F., Boucher, J., & Colson, R. H. (2001, November). Business continuity plans for disaster response [Electronic version]. ***CPA Journal*****, 60-60.**

Abstract: This article focuses on an effective strategy for business continuity in response to the terrorist attacks in the United States on September 11, 2001. It discusses the industries affected by the disaster, risks faced by the organizations, benefits of an effective strategy for business continuance, information on disaster recovery plans, and resulting changes in continuity planning.

Comments: This article helps frame DR planning for IT systems within the larger context of business continuity planning. It also discusses reasons why planning for disasters is important for businesses and cites primary research performed by a large market analysis company, Gartner Group, for support. This article is evaluated to be credible because it is published in a peer-reviewed journal, it cites primary research, and the author is an executive with a DR planning organization.

Bradbury, C. (2008). Disaster! [Electronic version]. ***British Journal of Administrative Management,*** **14-16.**

Abstract**:** This article discusses strategies for maintaining and repairing information technology (IT) services in the wake of a disaster. The author discusses the design of disaster recovery plans (DRP) to ensure business continuity management (BCM) in the event of a disaster. The article notes the importance of backing up IT files and ensuring that planned recovery point objectives (RPO) are met within the maximum tolerable period of disruption (MTPD). Diagrams illustrate the disaster assessment and recovery process, and note the importance of testing disaster recovery infrastructure.

Comments: This article identifies the key elements of DR planning and includes a discussion of how to conduct planning activities. It also lists objectives that should be established when performing DR testing. This information speaks directly to the purpose of this literature review. The credibility is assured because the author is a senior business continuity consultant and the article is published in a peer-reviewed journal.

Cerni, L. (2006). ***Building a comprehensive disaster recovery plan*****. Retrieved November 16, 2008, from Disaster Recovery Journal: http://www.drj.com/index.php?option=com_content&task=view&id=888&Itemid=429**

Abstract: "Disaster recovery has been top-of-mind for many IT managers as events that cause unplanned business downtime continue to surprise us; 2005 was no exception. Natural disasters, human conflicts and constant exposures to security breaches and attacks have driven organizations of all types and sizes to recognize the need to

implement or improve their comprehensive business continuity plan (BCP) that includes a robust IT disaster recovery plan." This article suggests that IT should do the following when planning for disasters: Understand and communicate the need for DR planning, implement DR plan, and maintain control by revising the plan as the environment changes.

Comments: This article provides a detailed list of leading questions that can be used to develop a DR plan. It also cites a study of 500 IT managers by Applied Research and highlights results such as the finding that cost is the largest barrier to DR projects. This information helps to identify the key factors that must be considered when developing a DR plan and identifies barriers that must be overcome. The article is usable within this literature review since its author is a professional business continuity director and it is published on a peer-reviewed journal's Web site.

Chisholm, P. (2008, July). Disaster recovery planning is business-critical [Electronic version]. *CPA Journal*, 11-11.

Abstract: This article offers tips for information technology (IT) disaster recovery planning. It suggests developing a disaster recovery plan and considering it as a document that must be updated frequently. It advises companies to utilize an offsite, secure data storage center as part of setting up a backup data solution. The author recommends recruiting managed services providers (MSP) to handle disaster recovery projects.

Comments: Although it is brief, this article offers a consolidated list of tips for consideration when developing a disaster recovery plan. The guidelines presented in this

article are useful because they identify key DR planning steps and the order in which the steps should be performed. It also cites statistics on disaster vulnerability from Info-Tech Research Group that will support the argument that DR planning by businesses is a necessary investment. This article is written by the CEO of a managed IT services company who has a background in DR planning. In further support of its credibility, the article cites primary research and is published in a peer-reviewed journal.

Clas, E. (2008, September). Business continuity plans [Electronic version]. ***Professional Safety,*** **45-48.**

Abstract: This article offers information on the survey made by Hewlett-Packard Co. on the importance of continuity plans in business in the U.S. A business continuity planning states that risk managers are looking at ways to protect company assets in the time of crisis, financial managers are looking to ensure that accounts payable and receivable would be handled after an event and human resource managers are looking at ways to protect jobs. Thus, to achieve business continuity management (BCM), one must establish the need of BCM program, including resilience strategies, recovery objectives, risk management considerations and crisis management plans, and develop and document the action plans to facilitate communication of critical continuity information.

Comments: Clas' article illustrates problems that can afflict business continuity planning, describes the lack of universal standard for BC planning techniques, and identifies ten "essential" elements of BC management. While it does not speak specifically about IT DR, many of the preparation steps that the article describes, such as program management and risk evaluation, apply to IT DR. The article is evaluated to be a good

source for this literature review since the author is an executive at an emergency management company and it is published in a peer-reviewed journal.

Conz, N. (2008, January 1). Preparing for the worst [Electronic version]. ***Insurance & Technology*****, pp. 30-36.**

Abstract: This article explains that to maintain operations and service levels in the face of a catastrophe, insurers increasingly are viewing disaster recovery plans as full-fledged business initiatives that must be constantly updated to account for new developments. The author emphasizes the need to identify time-critical systems and ensure that those are the first to be restored. However, the author cautions that "sometimes the threat of catastrophe - and accompanying precautionary evacuations - can be just as disruptive from a workforce perspective."

Comments: Conz provides a description of "time-critical" systems within the context of disaster planning that is used as a definition within this literature review. The article also provides evidence to suggest that disaster recovery plans should be maintained regularly, which is one of the key elements of a DR plan identified in this review. This resource is considered to be credible because it is published in a peer-reviewed journal and cites experts within the field of disaster recovery planning.

De Tura, N., Reilly, S. M., Narasimhan, S., & Yin, Z. J. (2004). Disaster recovery preparedness through continuous process optimization [Electronic version]. ***Bell Labs Technical Journal*****, 147-162.**

Abstract: When the news of the attacks on the World Trade Center and the Pentagon came in on September 11, 2001, Lucent Technologies program managers for each of the

major telecom customers in the New York/Washington, D.C., area were in contact, beginning the arduous process of support and recovery for one of the worst disasters in the history of the world. This article describes how the advanced disaster recovery planning that had been put in place for such an unthinkable event gave the customer emergency center teams, led by a certified program management staff, a map to guide them through the days ahead.

Comments: The case study in this article illustrates the need for DR planning activities to be performed in an iterative process. This explanation is used to develop the DR plan maintenance best practices within this literature review. Additionally, De Tura et al. provides a definition against which is measured the notion of "key element" as defined in this study. The article's credibility is established by the inclusion of bibliographic information and its having been published in a peer-reviewed journal that focuses on information technology systems.

Decker, A. (2005, January). Disaster recovery: what it means to be prepared [Electronic version]. *DM Review,* 44-46.

Abstract: This article discusses the adoption of business continuity management to minimize the effects of disasters on business enterprises. Today, disasters can result from terrorist attacks, power outages, security breaches, nature and human error. With the heightened threat of such disasters, there is an increased risk of business disruptions. Business disruptions resulting from disasters plague more than 90 percent of all businesses. The only way to minimize the effects of these disasters is to have an implemented business continuity plan.

Comments: This source establishes the context of a DR plan within the broad subject of business continuity planning. It also provides statistics to indicate that (a) most businesses will experience a disaster, (b) that companies that are unprepared are likely to close within five years, and (c) that the failure of critical IT systems can increase the odds of business closure. This article's quality is deemed to be sufficient due to the author's position as the executive director for an information security company and the article's publication in a peer-reviewed journal.

Gondek, R. (2002). When more of the same isn't better [Electronic version]. ***Journal of Business Strategy,*** **16-18.**

Abstract: This article reports on the impact of the September 11 terrorist attacks on the on information technology community in the United States, including allocation of disaster recovery to the system recovery site, importance of business continuity planning, and assessment of the information technology disaster project.

Comments: This article describes several DR planning key elements identified within this literature review, including those involving test methodologies, plan maintenance, and resource allocation. It further indicates that the terrorist attacks of September 11, 2001, forced many companies to activate and subsequently revise disaster recovery processes. The fact that processes changed after 9/11 is the reason that this literature review limits the age of its resources to those written after the terrorist attacks. This is a good resource for this literature review because the author is an experienced IT professional with a network engineering and consulting firm. It is also published in a journal that subjected the article to a peer-review process.

Gregory, P. H. (2008). ***IT disaster recovery planning for dummies.*** **Hoboken: Wiley Publishing, Inc.**

Abstract: This book describes how to get started with IT disaster recovery by creating a safety net while working out the details of a major plan. According to the author, the right plan will get a business back on track quickly, "whether it is hit by a tornado or a disgruntled employee". The book provides recommendations about how to assess a company's IT environment, develop both short-term and long-term plans, validate plans through testing, and keep disaster recovery plans updated.

Comments: Many of the procedures outlined in this book are used to identify DR planning stages and subtopics within this literature review. The author also provides an explanation about the role of disaster mitigation in recovery planning. The author holds certifications from reputable technology industry organizations including ISACA and $(ISC)^2$, and has written fifteen books on security and technology. His qualifications as an expert in the field are further supported by his professional role as an IT security strategist for a publically traded software company.

Jrad, A., Morawski, T., & Spergel, L. (2004). A model for quantifying business continuity preparedness risks for telecommunications networks [Electronic version]. ***Bell Labs Technical Journal*****, 107-123.**

Abstract: According to the authors, the need for disaster recovery has always existed. However, the emphasis is shifting from reactive (recovery) to proactive (preparedness) to minimize damage from disasters and limit disaster impact through proper planning. This article presents a new model for business continuity preparedness (BCP) planning for

telecommunications networks and a taxonomy for the quantification of the BCP readiness compared to similar businesses and industry practices.

Comments: This study establishes that disaster recovery planning techniques changed after September 11, 2001. This is the deciding factor used to limit resources for this literature review to those published after August, 2001. The article also describes a model that one industry should use to identify and protect time-critical IT systems while avoiding excessive costs. The credibility for this article is established by its publication in a peer-reviewed journal, its inclusion of references to prior work, and the experience attributed to its authors in the fields of business continuity and business modeling.

Lesser, A. (2004). Pre-testing DR plans to avoid business interruption [Electronic version]. ***Disaster Recovery Journal,*** **70-72.**

Abstract: According to the author, effective IT disaster recovery (DR) and business continuity planning is essential for every business. All businesses depend on their IT services for moment-to-moment operations. So they must all take measures to ensure that those services are not disrupted due to a natural or man-made disaster. This article explains that pre-testing DR plans in simulated network environments can help overcome challenges associated with DR planning.

Comments: This article identifies specific challenges, cited within this literature review, that afflict DR planning initiatives. To overcome those challenges, the article also describes techniques in DR plan testing that assist this literature review's identification of best practices. The resource is considered credible due to its author's experience with IT

engineering and security as well as the article's publication in a peer-reviewed journal with specific focus on the field of disaster recovery planning.

North, E., North, J., & Benade, S. (2004). Information management and enterprise architecture planning - a juxtaposition [Electronic version]. ***Problems & Perspectives in Management,*** **166-179.**

Abstract: This exploratory report juxtaposes overviews and key concepts pertaining to information management and enterprise architecture planning. Neglecting the management of information as an organizational resource may be the reason for the poor understanding towards information architecture as a critical component of the total enterprise architecture. The authors view the enterprise architecture approach as a window of opportunity in terms of educating senior managers on the value of information management practices.

Comments: This article establishes the connection between the field of information management and the need to protect information assets. The connection helps to describe the larger context within which DR planning resides. Furthermore, this literature review bases its definition of information management on the way in which the subject is described by North et al. The resource is considered credible in that the article is published in a peer-reviewed journal and provides extensive bibliographic information.

Rothstein, P. J. (2007). ***Disaster recovery testing.*** **Brookfield: Rothstein Associates.**

Abstract: This book emphasizes the importance of testing DR plans. It discusses the "necessary management skills, effective use of resources, and the elements of successful testing in various settings." The initial chapters address general disaster recovery

planning techniques "including how to justify, budget, and manage the process – but all are geared towards testing." Furthermore, "the authors provide numerous checklists and suggest topics to cover in any disaster recovery planning document."

Comments: This resource describes best practices for DR plan testing in great detail, which is valuable in the development of this guide's "Testing a DR Plan" section. The textbook helps to integrate testing with other DR planning activities by establishing testing within the context of other key elements to DR planning. The primary source of the book's credibility is its authors: 30 disaster recovery professionals wrote it jointly. The book also provides bibliographic citations to previous publications, which indicates that it is a scholarly resource.

Ryan, J. J., & Ryan, D. J. (2005, February). Proportional hazards in information security [Electronic version]. ***Risk Analysis: An International Journal*****, 141-149.**

Abstract**:** Ryan & Ryan explain that nonparametric methods can be used to analyze failure times and estimate probability distributions for failures of systems due to successful attacks on confidentiality, integrity, and availability in information security. However, such methods do not take full advantage of supplemental information regarding the configurations of systems in an information infrastructure that is usually also available. By correlating system survival times to the use of specific design enhancements and security countermeasures, as well as to system exposure based on choice of operational functionality, guidance can be obtained for making investments in information security.

Comments: This article establishes the link between information availability, of which DR is a component, to information security. It also provides a description of other information security concerns for which information security professionals are responsible. This article is published in a peer-reviewed journal and provides extensive references to prior work, and thus it is deemed to be a good resource for this literature review.

Snedaker, S. (2007). *Business continuity & disaster recovery for IT professionals*. Burlington: Syngress Publishing, Inc.

Abstract: This book provides complete coverage of the three categories of disaster: natural hazards, human-caused hazards, and accidental/technical hazards. It addresses many types of risks, such as cyber attacks, rioting, protests, product tampering, bombs, explosions, terrorism, and natural disasters. Included are extensive disaster planning and readiness checklists for IT infrastructure, enterprise applications, servers and desktops. The author offers clear guidance on developing alternate work and computing sites and emergency facilities, as well as actionable advice on emergency readiness and response.

Comments: Snedaker's explanation of how to conduct DR planning activities for business IT systems helps to structure and inform the key elements identified within this study. The planning steps suggested in the book weave together concepts illustrated in other resources, and the book plays a key role in the development of this guide's DR planning framework. The case studies included in the book are also used to identify best practices. This is a trusted resource due to the author's extensive professional and academic experience with the strategic management of IT resources. The book also

credits contributions from other professionals in the field of business continuity, disaster recovery, and crisis communications.

Spencer, R. H. & Johnston, R. P. (2003). *Technology best practices.* Hoboken: John Wiley & Sons, Inc.

Abstract: According to the authors, Technology Best Practices offers nontechnical managers a forward-thinking blueprint for implementing effective and efficient technological programs, as well as for weaving technical personnel into the managerial process. The chapter on IT disaster recovery planning describes important design plans that cover a wide variety of potential failures. It emphasizes the importance of prioritizing recovery activities based on the level of risk faced, and allocating enough resources to ensure that companies can successfully return to pre-disaster levels.

Comments: This book is cited heavily as a resource for the DR best practices identified within this literature review. It provides in-depth instructions on how companies should conduct DR planning activities, such as a Business Impact Analysis, and how IT systems should be prioritized during a recovery initiative. The authors cite over 60 years of combined experience in IT management as well as consultations from other subject matter experts in order to assert credibility of the prescribed best practices.

Teuten, P. C. (2005, September). The top ten mistakes in risk management [Electronic version]. *Financial Executive,* 45-45.

Abstract: This article presents common mistakes made by businesses pertaining to risk management. According to the author, many companies ignore the element of risk that exists within every business practice. Experts say organizations should undergo a

comprehensive risk assessment by independent experts. Organizations often fail to understand the consequences and long-term business impact of risk. Simply buying insurance as a means of risk management is a common error. There are many tools and services that are needed to manage risk including disaster recovery plans, anti-virus software, intrusion detection, and firewall technologies.

Comments: The top-ten list of mistakes included in this article explains that the assumptions companies use to postpone or under-fund disaster preparation are incorrect. Identifying fallacies from the list in this literature review helps to justify DR expenditures, thus removing obstacles to DR planning. This resource is judged to be credible because the author is an executive with a risk management organization and it is published in a peer-reviewed journal.

Toigo, J. W. (2003). ***Disaster recovery planning: preparing for the unthinkable.*** **Upper Saddle River: Prentice Hall PTR.**

Abstract: In this book, Toigo offers focused, hands-on blueprints for disaster recovery in every environment, centralized and decentralized – with detailed coverage of building DR systems that address networks and encompass end-users who still maintain crucial enterprise data on local PCs and notebooks. Thoroughly revised to reflect the latest strategies and technologies, this book presents the disaster recovery lessons taught by 9/11, the California energy crisis, and the anthrax scare.

Comments: This book provides details about the requirements and components of IT DR plan development, which is valuable to the identification of best practices in this review. The book's discussion of how a lack of DR planning standards complicates development

is cited to establish the problem that is addressed by this literature review. Credibility for the textbook is established by the author's experience of having developed over 60 disaster recovery plans for commercial and governmental clients. Furthermore, the inclusion of bibliographic information suggests that the book is a scholarly resource.

Weiner, S. (2001). Managing effective disaster recovery [Electronic version]. ***CPA Journal,*** **22-26.**

Abstract: Weiner's article discusses the elements that should be considered in the development of disaster recovery plans for businesses. Those elements include the organization of the crisis management team, identification of unique exposures to the organization that require special preparation, procedures of crisis management, and business recovery procedures.

Comments: This article identifies strategic factors, cited within this literature review, which should be addressed when preparing for disasters. It also explains that the problems with BC management, and consequently DR planning, lie in the cost and complexity. As a result, Weiner explains, many organizations have an inadequate BC plan or no plan at all. This is judged to be a good resource for this literature review due to the author's experience with DR planning for his own organization and the article's publication in a peer-reviewed journal.

Wells, A., Walker, C., & Walker, T. (2007). ***Disaster recovery principles and practices.*** **Upper Saddle River: Pearson Prentice Hall.**

Abstract: With real world examples, this text provides an extensive introduction to disaster recovery focusing on planning the team, planning for the disaster and practicing

the plan to make sure that, if ever needed, it will work. In addition to discussing the key elements of disaster recovery plans, the book includes a sample disaster recovery plan as well as checklists that can be used for DR plan validation.

Comments: This book plays a central role in identifying the composition of key DR planning elements cited within this literature review. The resource is particularly valuable to this guide due to its depth in describing how to conduct key planning activities including risk assessments, impact analyses, plan testing, and ongoing maintenance. The authors are evaluated to be credible since they each have extensive professional experience conducting DR planning activities, managing IT systems, and training other IT professionals and school faculty on related subjects.

Review of the Literature

Keyword searches through online indices and library resources indicate that there is a large volume of information published on the subject of DR planning for business IT systems. The selected literature reveals that, while experts generally agree on the activities required to develop a DR plan, each expert chooses to break up those activities differently. The major DR planning activities are divided into as few as three (Gregory, 2008, p. 2), or as many as ten (Clas, 2008, p. 47) distinct categories. This review of literature organizes the major activities into five stages that are based on the models proposed by Spencer & Johnston (2003, p. 90), Snedaker (2007, p. 32), and Gregory (2008, p. 2). The five DR planning key stages identified in this literature review include Project Initiation, Conducting a Business Impact Analysis, Developing a DR Plan, Testing a DR Plan, and Maintaining a DR Plan.

Key stages are first described and then explicated with information derived through the data analysis process conducted on selected literature, including expert suggestions, best practices, and case studies. This section of the study is structured as a guide that details DR planning activities in which businesses should engage to protect time-critical IT systems from potential disasters.

Stage 1: Project Initiation

Several leading business continuity organizations from the United States and the United Kingdom have published DR planning guidelines that suggest an initiation process in which the need for a business continuity program is established, management support is obtained, and a project plan is defined (Clas, 2008, p. 47). Snedaker (2007) warns that without conducting an effective project initiation process, a DR strategy will be incomplete and potentially unsuccessful

when activated (p. 33). For example, an IT professional who attempts to develop a DR plan without engaging other subject matter experts and managers will not be able to accurately assess the time-critical systems or the needs of each relevant stakeholder (Snedaker, 2007, p. 33).

This section outlines the activities that organizations should consider when first embarking on a DR planning initiative. The selected literature presents these activities in varying order, which suggests that the sequence in which the activities are conducted varies from one organization to another, depending on circumstances, without causing a significant impact to the outcome.

Securing management support. As Gregory (2008) explains, DR planning projects disrupt business operations by pulling staff members away from their regular duties for an activity that does not obviously or directly provide revenue or improve efficiency (p. 15). Securing management support can be a daunting task since business executives typically require strong evidence that there will be a return on resource investments (Gregory, 2008, p. 15). Snedaker (2007) suggests that the best approach is to speak from a business standpoint in plain language that is free of technical jargon (p. 57). The goal is to show management that DR planning supports (a) disaster preparation and survival, (b) disaster avoidance, and (c) due diligence and due care to protect against costly losses (Gregory, 2008, p. 16). According to Swartz (2003), documenting these critical business needs should encourage senior management to confront and demand “honest answers to a vital question: Is the organization prepared to withstand a major disruption?” (p. 7).

Organizing the planning project team. In order to be effective, the DR planning team must include empowered decision makers and those “who know what data and business

processes" are time-critical and require swift recovery in the event of a disaster (Chernicoff, 2007, p. 49). Wells et al. (2007) emphasizes that since every business unit within an organization knows its own functions and idiosyncrasies best, representatives from each should be considered essential members of the DR planning team (p. 31). In addition to collaborating on the development of an initial DR plan, the team will remain intact to oversee the ongoing maintenance of the plan. If an organization experiences difficulty selecting members to join the DR planning team, Snedaker (2007) suggests that a preliminary project team be created that is tasked with the creation of a basic project definition and the selection of the permanent planning team members (p. 72).

An important consideration for DR planners, suggests Wells et al. (2007), is that they may not be involved in an actual recovery effort if a disaster takes place (p. 30). In fact, depending on the size and security concerns inherent to an organization, it is often better to separate the planners from the response team to provide a degree of external oversight to the process (Teuten, 2005, p. 45). DR planners should include enough detail about their area of responsibility to enable whomever is testing or conducting an actual recovery effort to perform the specified tasks with precision and accuracy (Wells et al., 2007, p. 31).

Establishing the project management process. According to the selected literature, DR experts agree that planning initiatives should adhere to formal project management processes. As Snedaker (2007) explains, an experienced project manager can be essential to the development of a clearly defined DR planning process (p. 63). Such individuals can often bring a set of "methods, procedures, and associated documents" to the planning effort that they had used effectively in the past (Snedaker, 2007, p. 63). The project manager will often report to a board

of directors and/or senior management who can issue or withhold approval and retain the ultimate responsibility for the plan's development (Spencer & Johnston, 2003, p. 90).

Regardless of the specific process agreed upon by the project manager and senior management, it is best to begin a DR planning effort with a kickoff meeting that can last, as suggested by Gregory (2008), up to three hours (p. 18). The goal of the kickoff meeting is to align all of the project's stakeholders to the same objective and to begin to build familiarity and trust between team members. For the kickoff meeting to be effective, representatives for all parties involved in the project should be included (Gregory, 2008, p. 18) (also see *Organizing the planning project team* above).

Obtaining the required resources. As Cerni (2006) states, a common reason that many organizations do not have a DR plan in place is a lack of resources. Business executives withhold resources due to the assumption that the risk and potential costs of a disaster are not sufficient to justify the costs required to develop a recovery plan and put backups in place for time-critical IT systems (Teuten, 2005, p. 45). Cerni (2006) suggests that this barrier can be overcome by effectively communicating that "the cost of developing a disaster recovery plan can be quite low, relative to the impact on recovery" (para. 8) (also see *Organizing the planning project team* above).

Toigo (2003) suggests two strategies that are commonly used to overcome financial obstacles (p. 16). These strategies align with the approaches cited in the *Securing management support* section (see above), since according to Snedaker (2007), management controls the dissemination of resources throughout an organization (p. 55). The first strategy suggested by Toigo (2003) is to calculate the total average hourly cost for workers who are unable to produce

during the downtime, including the overtime needed to make up the work later (p. 17). This approach can be strengthened by citing known replacement costs for damaged systems along with intangible costs such as lost sales, damaged customer satisfaction, or potential legal liabilities (Toigo, 2003, p. 17). Snedaker (2007) advises that DR planners can work with individuals in other departments such as finance to estimate potential benefits (p. 57).

The second strategy that Toigo (2003) outlines is to "demonstrate the collateral benefits" of a DR plan (p. 17). Having an effective DR plan in place can reduce insurance costs for some organizations (Toigo, 2003, p. 17). Furthermore, a DR plan can lead to environmental changes such as the investment in battery backup systems that save money by extending the useful life of production equipment (Toigo, 2003, p. 17). Gregory (2008) adds that DR planning can also result in improvements to processes and technology that reduce system outages and improve service quality (p. 13). Individuals in the operations or facilities departments may be able to furnish information for estimates regarding these collateral benefits (Snedaker, 2007, p. 57).

The responsibility for inadequate resources being directed toward DR planning does not always lie with business executives. Gondek (2002) points out that in the event that IT organizations get additional funding, IT staff members "most often look at upgrading their current capabilities" rather than embarking on DR planning initiatives (p. 18). Statistics that most companies experience a disaster and many fail to recover (Decker, 2005, p. 44) can be used to direct IT staff members to channel additional funds in specific support of a DR planning project.

Developing initial project objectives. Specifying objectives at the onset of a DR project will help define parameters for the endeavor (Gregory, 2008, p. 17) and guide the efforts of the planning team. The objectives for a DR plan can be narrow or wide, depending on a company's

size and composition (Snedaker, 2007, p. 75). Although it is reportedly a good idea to specify objectives early in the planning process, initial objectives can be revised if the need to do so is identified subsequently during the business impact analysis (Bradbury, 2008, p. 16). Table 4 (see below) illustrates some of the key objective categories and examples, identified by Toigo (2003), which should be addressed in a DR project plan (p. 55):

Key objective category	Example DR objective
Plan maintenance	Develop a schedule for periodic review and maintenance of the DR plan.
Physical environment	Collect information regarding company facilities to assess the susceptibility to a disaster.
Organizational control	Develop a formal ownership program to assign the responsibility for recovering each time-critical system to individual employees.
Systems and networks	Develop the capability to recover each time-critical system within an acceptable timeframe.
Backup/off-site storage	Identify the resources that should be backed up to an offsite location and specify a schedule and method for the process.
Emergency action	Document the notification procedure that will be used to alert the disaster response team if the DR plan is activated.

Table 4: Example objectives that can be specified within a DR plan

The objective categories specified in Table 4 are not exhaustive, and each one could be replaced with similarly defined objectives (Toigo, 2003, p. 54). While identifying objectives for a specific project, the selected literature suggests that the DR planning team should focus on creation of context-relevant categories to address three overarching goals: (a) prevent a disaster from taking place, (b) maintain preparedness, and (c) speed the recovery of time-critical IT systems after a disaster takes place.

Stage 2: Conducting a Business Impact Analysis

A Business Impact Analysis (BIA) is a study of an organization's IT systems that aims to determine which resources warrant the expense and effort of distinct inclusion in a disaster recovery plan (Gregory, 2008, p. 51). A BIA further specifies the priority by which each time-critical system is recovered after a disaster (Bradbury, 2008, p. 16). The close examination of technology and business processes necessitated by a BIA can also identify potential changes that will reduce system interruptions or improve service quality (Gregory, 2008, p. 13).

An assessment of current literature indicates that the creation of a BIA is a best practice that should play a central role in DR planning activities. However, according to Drummond (2008), a recent survey of business continuity managers reveals that 20 percent of businesses with continuity plans do not have a current BIA on file, and one third of those companies with a BIA have failed to keep it up to date. The key DR planning activities identified within this stage specify the tasks that businesses should perform when creating or updating a BIA.

Gathering information. Snedaker (2007) explains that there are four primary ways of gathering information for a BIA: (1) questionnaires, (2) interviews, (3) documents, and (4) research (p. 231). DR planners should consult with management staff, subject matter experts (Gregory, 2008, p. 55), and internal auditors (Barrier, 2001, p. 58) to determine the types of information to seek and where it may be found. Snedaker (2007) suggests that these individuals be sought out using a company's organizational chart or, if one is not available, the internal telephone directory (p. 232). The information gathering process should be systematic, notes Gregory (2008), in order to make certain that the same results would be received regardless of who actually performs the analysis (p. 58).

A descriptive sample of individuals who use the business' IT systems should also be surveyed to help determine what is considered to be time-critical. As Ulfelder (2004) explains, DR planners often neglect to seek input directly from users about which IT systems and applications are needed most. However, Toigo (2003) warns that businesses should proceed with caution since it is common for users to respond that all of the systems with which they work are time-critical (p. 40). To mitigate this potential problem, the criteria used to classify the importance of each system should be clearly explained (Toigo, 2003, p. 40). Furthermore, DR planners should strive to canvass users regarding the steps that would be required to work around a failed IT system rather than simply to rate its criticality (Toigo, 2003, p. 40).

Identifying the time-critical IT systems. According to Conz (2008), time-critical IT systems are comprised of the technology on which key business processes rely and that must be "specifically prioritized" for prompt recovery after a disaster occurs (p. 32). For each of the systems identified during the *Gathering information* process (see above), DR planners must compile and analyze the available information to gauge its relevancy. To help businesses identify which IT systems are in fact time-critical, Snedaker (2007) suggests that businesses first identify processes that are most critical, such as those that involve customer, regulatory, or operational issues, and then correlate that information with the IT systems that have been identified (p. 243).

In addition to determining which systems are time-critical, it is also essential to track the location of those systems. As Wells et al. (2007) explains, the assets that must be tracked include hardware, software, and electronic data (p. 114). Hardware includes physical assets that make up a computer system such as network servers and storage devices (*Hardware*, n.d.), and can be tracked using a database or spreadsheet application (Wells et al., 2007, p. 108). Software is an

electronic set of carefully organized instructions that must be installed on the hardware in order for that hardware to function (*Software*, n.d.). Wells et al. (2007) warns that although software can be tracked similarly to hardware, organizations should be careful to also document any customizations that have been made to key software after the point at which it was installed (p. 112). Electronic data comprises the digital information that has been manipulated software (*Data*, 2003). According to Chernicoff (2007), electronic data must be accessible in order for many IT systems to provide value (p. 49). Although data is often stored within an organization, it can also be stored externally (Wells et al., 2007, p. 108), in which case the systems required to connect to the external data source must also be outlined within the DR plan.

Performing a risk assessment. In addition to gathering information about time-critical IT systems, DR planners should also meet with key members of the company, such as those responsible for facility management, to analyze the potential risks with which the company is faced (Snedaker, 2007, p. 33). Snedaker (2007) explains that such risks could include concerns ranging from a fire or flood in an IT server room to a major earthquake or hurricane that destroys entire facilities (p. 33). Secondary effects of disasters, notes Gregory (2008), such as utility and communication outages, should also be considered as potential risks (p. 67).

Gregory (2008) outlines a formal approach that organizations can follow to identify and prioritize the risks that could lead to a disaster (p. 68). The approach includes the following steps: (1) identify each potential disaster that could affect time-critical IT systems; (2) assign a value between 1 and 10,000 that represents the likelihood of each disaster, with 1 being the least likely to occur; (3) for each disaster identified, rate the potential impact on the time-critical IT systems, again using a scale of 1 to 10,000; (4) multiply the likelihood values by those estimated

for the impact; and (5) sort the results to list the risks with the highest calculated numbers, representing the most significant risk, first (Gregory, 2008, p. 69). The broad range of values allows companies to distinguish clear priorities between many potential risks. Table 5 (see below) provides an example of this prioritization process:

Potential risks to time-critical IT systems	Likelihood of disaster	Impact on time-critical systems	Calculated priority (likelihood x impact)
Flood in IT data center	1,500	6,000	**9,000,000**
Loss of power that exceeds 24 hours	1,000	7,500	**7,500,000**
Virus attack on enterprise network	4,000	1,000	**4,000,000**
Hurricane destroying company headquarters	250	10,000	**2,500,000**
Denial of service attack on corporate Web site	2,000	750	**1,500,000**

Table 5: Example prioritization of risks that face time-critical IT systems

The disasters included in Table 5 are only a sample and may not be relevant to all businesses due to differences in each organization's composition and geographic location. For example, in the natural disaster category, a business located along the southern coastline of the United States might be highly susceptible to hurricanes, while tornados may be of more concern to businesses located in the American Midwest (Spencer & Johnston, 2003, p. 92).

Prioritizing the recovery efforts. After identifying time-critical IT systems and potential risks that may result in outages, DR planners should systematically allocate resources and prioritize the recovery of each time-critical IT system (Teuten, 2005, p. 45). The DR planning team should focus its resources on the IT systems that are evaluated to be the most critical and the most at risk. Identifying recovery priorities during the planning process, notes Bradbury

(2008), will prevent paralyzing discussions about the order in which system recovery should take place after a disaster has occurred (p. 16).

According to Wells et al. (2007), it is not possible to recover all time-critical IT systems simultaneously due to a limited supply of resources (p. 72). Faced with this reality, Chisholm (2008) recommends that businesses define clear objectives to prioritize recovery operations and establish how much information can afford to be lost from each system due to the outage.

The first step in the prioritization process is to define a maximum tolerable downtime (MTD) for each time-critical IT system that specifies how long the business can function after the system fails (Gregory, 2008, p. 72). Next, the business should calculate a recovery time objective (RTO) that declares how quickly the system should be restored (Bradbury, 2008, p. 14). The RTO must be less than the MTD to account for delays in the resumption of work after a system outage (Snedaker, 2007, p. 219). The final step in the prioritization process is to create a recovery point objective (RPO) that identifies the amount of information that a business can afford to lose permanently from each system during a disaster (Bradbury, 2007, p. 14). The RPO will determine how frequently electronic data must be backed up to an offsite location from which it can subsequently be restored after a disaster has taken place (Snedaker, 2007, p. 219).

Stage 3: Developing a DR Plan

According to Spencer & Johnston (2003), the development of an appropriately detailed recovery plan is the most important aspect of DR planning (p. 94). To adequately respond to a disaster, Spencer & Johnston (2003) continue, a business must have a "well thought-out, documented" DR plan in place (p. 94). An analysis of the selected literature on DR planning best practices indicates that it is during the development stage that organizations specify (a) how to

react to disaster scenarios, (b) when to activate a DR plan, (c) how each critical IT system should be recovered, and (d) who should perform needed recovery tasks. The key elements identified within this section can guide DR planners as they develop and document recovery strategies based on information identified through the BIA process described in Stage 2 (see above).

Selecting the risk management strategies. As indicated by Cerni (2006), businesses should develop a management strategy to address each of the risks identified during the BIA process (see *Performing a Risk Assessment* in Stage 2 above). Cerni (2006) suggests that for each potential risk, DR planners must decide to: (a) accept the risk, (b) transfer the risk to a third party, or (c) work to reduce the company's exposure through risk mitigation. As Snedaker (2007) explains, companies may choose to accept a risk, i.e. take no action, when the cost of transfer or mitigation exceeds the potential cost of the risk itself (p. 264). Transfer to a third party involves either outsourcing a particular process or purchasing insurance to cover potential losses (*Risk transfer*, n.d.). Risk mitigation involves taking steps to systematically reduce the adverse effects of an event such as a disaster (*Risk mitigation*, n.d.). These steps can include making modifications to an environment to avoid or reduce the impact of a potential risk (Snedaker, 2007, p. 265).

Defining disaster severity levels. As Chernicoff (2007) notes, planning teams should specify the severity of disasters that will be addressed within a DR plan. Spencer & Johnston (2003) suggest that a best practice approach is to define potential failures, divide them into levels, and then prepare recovery strategies to address each level (p. 99). A quick categorization approach is to define minor, intermediate, and major disaster levels, each with its own DR strategy (Snedaker, 2007, p. 297). Companies with complex environments that require more

detail can identify three or more levels of failures, with severity based on (a) the impact of an outage, (b) the time needed to recover, and (c) the number of people affected (Spencer & Johnston, 2003, p. 99).

Spencer & Johnston (2003) note that although DR plans have historically focused on disasters with high severity levels, the cumulative loss from small technology failures can be greater than the loss from a single catastrophic event (p. 99). As a result, Spencer & Johnston (2003) recommend that DR planning teams develop recovery strategies for disasters at each severity level with the same degree of diligence (p. 99).

Identifying activation triggers. The selected literature describes two primary methods that organizations can use to declare a disaster and commence the initiation of a DR plan. One method is to identify a core group of decision-makers within the organization who must assemble in the event of a disaster and come to an agreement about whether or not to begin recovery efforts (Gregory, 2008, p. 198). However, the difference between an inconvenience and a disaster, warns Wells et al. (2007), often depends on the perspective of those who are affected (p. 127). A printing problem that impacts a small group of people may be inappropriately designated as a disaster if those individuals are at risk of missing a deadline. While consensus about the need to activate a DR plan can be reached quickly when a major event such as hurricane takes place, grey areas such as the example printing problem can create costly delays in developing consensus among decision-makers (Lesser, 2004, p. 72).

The second method that organizations commonly use to declare a disaster, explains Gregory (2008), is to identify a uniform set of criteria by which each potential disaster is evaluated (p. 199). Snedaker (2007) suggests that identifying specific events, or “triggers,”

within each defined severity level can speed the activation of a DR plan during a crisis situation (p. 298). One of the best ways for organizations to identify triggers, according to Lesser (2004), is to conduct simulation testing with specialized software (p. 72). Simulation technology can show specifically how disasters will affect time-critical IT systems, and triggers can be developed based upon those observations (Lesser, 2004, p. 72).

After identifying activation triggers, Gregory (2008) recommends that DR planners develop a specific checklist of criteria, often in the form of a series of 'yes' or 'no' questions, which can be used by designated staff members when determining if a DR plan should be activated (p. 199). Individual questions can be weighted and assigned values, and activation can take place when the sum of all values answered 'yes' exceeds a predefined threshold. After a disaster of any severity level has been declared, the designated staff members would begin to notify members of the disaster response team to begin working through the procedures specified in the DR plan (Gregory, 2008, p. 199).

Defining and documenting specific recovery processes. Toigo (2003) stresses that, immediately following a disaster, the primary objective for companies is to replace the affected time-critical IT systems "quickly and by whatever means possible" (p. 120). To ensure that RTOs are met, Bradbury (2008) indicates that for each time-critical IT system, the DR plan should at a minimum specify (a) the recovery process and flow of activities, (b) high-level activities such as the installation of software and the restoration of data, (c) prerequisites and dependencies for each activity, and (d) a list of individuals who are responsible for each activity (p. 16). Each individual that is assigned a recovery task within the DR plan should document detailed recovery processes for that task, and the DR plan should refer to that documentation

(Bradbury, 2008, p. 16). By separating step-by-step recovery documentation and assigning its management to individual members of the disaster response team, DR plans will not require revision when minor changes are made to time-critical IT systems (Bradbury, 2008, p. 16).

In addition to high-level recovery processes and identifying the individuals who are responsible for each recovery activity, Spencer & Johnston (2003) suggest that two other lists be documented within the DR plan (p. 105). Both of these additional lists are intended to facilitate prompt communication of the disaster situation, which Pekala (2002) describes as a critical component of DR plans (p. 45). One list should include specific vendors, complete with contact information, which may need to be called upon in the event of a disaster (Spencer & Johnston, 2003, p. 105). The other list indicates key customers who may need to be notified of an interruption to services (Spencer & Johnston, 2003, p. 105). Customer notification may be necessary due to contractual obligations defined in a service-level agreement, or could alternatively serve to encourage patience and understanding.

Depending on the RTO developed for each time-critical IT system, the requirement may be specified for redundant hardware and software, as well as backup copies of corporate data, to be stored at an offsite location (Gregory, 2008, p. 155). The selected literature indicates that there are many alternatives for offsite system recovery. Table 6 (see below) lists those that are commonly considered during DR plan development:

Offsite recovery alternatives	**Description**
Hot backup site	A facility that is fully equipped to assume the responsibilities from damaged IT systems with little or no preparation but whose services can be costly (Gregory, 2008, p. 147). Organizations with multiple offices often implement hot sites by duplicating systems at two or more data centers (Wells et al., 2007, p. 148).

Offsite recovery alternatives	Description
Cold backup site	A leased building space that is used to setup temporary equipment to replace damaged IT systems (Wells et al., 2007, p. 146). Cold backup sites are inexpensive since they do not maintain backup equipment, but for that reason they can take "days to weeks" to activate after a disaster (Gregory, 2008. P. 148).
Warm backup site	A middle ground between hot and cold sites in regard to the cost and the time needed to activate after a disaster (Gregory, 2008. P. 148). Warm backup sites keep replacement hardware in stock but require software installation and data restoration prior to assuming the responsibilities from damaged systems (Gregory, 2008, p. 148).
Reciprocal agreements	Often a viable, less expensive alternative to a warm backup site, organizations can establish reciprocal agreements with another company to host each other's backup hardware (Wells et al., 2007, p. 147). Like warm sites, software and data must be restored after a disaster, delaying activation up to five days (Gregory, 2008, p. 148).
Vendor-supplied agreements	Organizations can establish agreements with vendors to provide and host replacement IT systems after a disaster (Wells et al., 2007, p. 149). However, Wells et al. (2007) cautions that organizations must be careful to evaluate whether potential venders can provide needed services fast enough to satisfy RTOs (p. 149).

Table 6: Alternatives for offsite system recovery

Wells et al. (2007) warns that the unpredictable nature of disasters can make it difficult for some organizations to identify an optimal offsite recovery solution (p. 149). Businesses in such a position should create a customized combination of recovery alternatives to satisfy those businesses' unique RTOs (Wells et al., 2007, p. 149). For example, companies located near an active fault line may establish a cold backup site in a different geographic area to protect against a major earthquake. However, that organization may also secure vendor-supplied agreements to enable the rapid recovery from less severe disasters that are more likely to occur.

Selecting disaster response team members. Weiner (2001) explains that successful disaster recovery "depends heavily on the managers and employees that have accepted

responsibility for specific areas of the plan" (p. 24). These individuals should be organized into a disaster response team composed of key management and staff members from throughout the organization who have the requisite expertise and authority to conduct the activities enumerated in the DR plan (Snedaker, 2007, p. 303). As reported by Spencer & Johnston (2003), a senior manager or executive should be appointed to lead the response team (p. 101). High-level individuals are ideal for this role, since they have the power to make resources available quickly during a disaster event. The team leader is also responsible for selecting other members of the response team and for ensuring that each team member is properly trained (Weiner, 2001, p. 24).

Stage 4: Testing a DR Plan

According to Twentyman (2008), the worst time to test a DR plan is during an actual disaster. Lesser (2004) warns that even when performing planned testing, it can be challenging for businesses to certify that the activities outlined in a DR plan will be successful once triggered (p. 70). However, Lesser (2004) continues, these challenges can be overcome by conducting effective tests to validate DR plans. Spencer & Johnston (2003) explain that validation tests should be designed to evaluate whether an organization can adequately satisfy the RTOs specified in its DR plan in the aftermath of a disaster (p. 95). In addition to accomplishing this fundamental task, Toigo (2003) suggests that testing can be used (a) as an audit tool to evaluate a plan and reveal shortcomings, (b) to benchmark the performance of recovery capabilities, and (c) to serve as a rehearsal to train response team members (p. 434). This stage outlines key elements that organizations should consider when attempting to validate the effectiveness of new or existing DR plans.

Developing a test strategy. Gregory (2008) cautions that DR testing requires a considerable amount of time and effort; therefore, organizations should develop a test strategy to maximize the use of testing resources (p. 219). The critical success factor in DR testing is not determining what systems to test, says Gondek (2002, p. 16); that information can be gathered with minimal difficulty from the recovery processes documented in Stage 3 (see above). Rather, the success of a DR test depends on the identification of key test objectives (Bradbury, 2008, p. 16) and the selection of effective test procedures (Gondek, 2002, p. 16). Bradbury (2008) explains that the test strategy should define the scope of testing procedures to ensure that tests will (a) verify the effectiveness of recovery procedures, recovery sites, and documentation; (b) familiarize the staff with recovery processes; (c) determine whether the RTOs are achievable; and (d) identify needed revisions to the DR plan (p. 16).

Training the recovery staff. As identified in Stage 3 (see above), the success of a disaster recovery effort depends on the effectiveness of the response team. For this reason, all individuals who are assigned a position in a DR plan should be included as regular participants in DR testing (Rothstein, 2007, p. 71). Rothstein (2007) explains that it is important to involve the response team in DR plan testing to give those individuals experiences that enable a “cool and competent” response to a disaster (p. 70). In addition to training through involvement in recovery testing, Spencer & Johnston (2003) suggest that other sources such as conference room training and seminar-based instruction should be utilized (p. 97). Teuten (2005) warns that if employees are not properly trained to implement a DR plan, the planning efforts will have effectively been “wasted” (p. 45).

Conducting the test procedures. Depending on an organization's culture and the preference of the response team leader, testing can be either spontaneous to simulate an actual crisis, or premeditated to encourage a "calm, rational" implementation of test procedures (Toigo, 2003, p. 243). However, explains Toigo (2003), neither method is necessarily superior (p. 435). Some organizations can chose to utilize both surprise and planned testing to give test participants experience with both approaches.

Regardless of the way in which a test is initiated, Toigo (2003) explains that there are many alternative methodologies and "the ones employed should be customized to the needs of a given business" (p. 434). Table 7 (see below) illustrates test methodologies that the selected literature indicates are most commonly in use, organized in ascending order and beginning with the methodologies that are the least complex:

Type of test	**Description**
Paper tests	Usually the first type of test to be performed, a paper test involves the review and revision of DR documentation by independent members of the response team (Gregory, 2008, p. 221). This is the least expensive methodology and catching problems at this point can prevent time from being wasted by unnecessarily conducting more complex testing methods (Gregory, 2008, p. 221).
Walkthrough tests	Also called a "talk through" test, walkthrough tests are a low-cost method that requires response team members representing each business unit to meet and describe the procedures that would be followed after a disaster takes place (Gondek, 2002, p. 17). According to Gondek (2002), descriptions should include the specific actions that would be taken within each business unit and identify external dependencies (p. 17) such as backup power provided by a diesel generator.
Simulation tests	Simulation tests attempt to duplicate entire network environments, to the extent possible, in a controlled laboratory environment (Lesser, 2004, p. 70). Due to the quantity and complexity of the systems involved, the development of simulations is often expensive and time consuming (Rothstein, 2007, p. 50). However, the resource investments can be justified since simulations create a "safe and flexible" environment in which time-

Type of test	Description
	critical IT systems can be evaluated under a wide range of possible scenarios (Lesser, 2004, p. 70).
Parallel tests	During parallel testing, members of the disaster response team perform the activities prescribed to them by the DR plan as if a disaster had occurred (Gregory, 2008, p. 227). However, these tests stop short of interrupting the services provided by the business' time-critical IT systems (Gregory, 2008, p. 228). For example, during a parallel test, replacement systems would be activated and data would be restored, but those systems would be kept isolated from the systems that are actually in use by the organization.
Cutover tests	This test methodology goes beyond parallel testing by requiring that time-critical IT systems be disconnected and replaced with backup systems that are developed by following the steps outlined in a DR plan (Gregory, 2008, p. 231). Few organizations can perform this test methodology because the voluntary interruption to key technology systems is perceived as too great a risk (Gondek, 2002, p. 17). However, Gregory (2008) suggests that cutover testing can foster confidence if customers and suppliers are notified prior to the beginning of the test (Gregory, 2008, p. 221).

Table 7: Test methodologies that can be used to validate a DR plan

Although many differences exist between test methodologies, each methodology shares a similar set of procedures that are required to organize the testing process (Toigo, 2008, p. 245). As stated by Gregory (2003), the common procedures between test methodologies are: (a) establish the purpose and type of test in advance, (b) define and document test objectives, (c) identify participants and observers, (d) schedule the test, (e) document the test results, and (f) conduct a revised test if the results are initially unsuccessful (p. 436). Gregory (2008) warns that, without incorporating these steps into a testing scenario, a test could incorrectly be judged successful while an actual recovery effort could fail (p. 221).

Establishing the test frequency. Business processes and the IT systems on which they depend change constantly, cautions Gregory (2008), and as a result, regular testing is required to verify that DR plans continue to remain effective (p. 236). Spencer & Johnston (2003) state that,

as a general rule, tests should be conducted on an annual basis. However, adds Snedaker (2003), "a quarterly or semiannual test may be prudent the first year" for organizations with a relatively new DR plan (p. 142). Gregory (2008) explains that organizations should weigh the following factors when determining how frequently to test a DR plan: (a) the cost of testing, (b) the severity of the risks identified in the BIA, (c) the frequency of changes to business processes or IT systems, (d), the degree of training required for disaster response team members, (e) demands by customers or business partners, and (f) any regulatory considerations that may apply (p. 237).

Stage 5: Maintaining a DR Plan

Teuten (2005) advises that due to the continuously changing nature of risks that face time-critical IT systems, businesses must ensure that DR plans are updated regularly to reflect the current environment (p. 45). Depending on the frequency and complexity of changes, explains Snedaker (2007), maintaining a DR plan "may end up being the biggest challenge" of the DR planning process for some businesses (p. 392). However, developing an explicit strategy to address DR plan maintenance can reduce the complexity of the task (Snedaker, 2007, p. 392). The final stage outlined in this review of DR planning literature describes discreet steps that organizations can perform to guarantee that DR plan maintenance remains pertinent and manageable.

Identifying potential sources of change. According to Toigo (2003), DR plans are "living documents that must grow and change" in response to transformations that regularly take place throughout an enterprise and the environment in which a business operates (p. 424). The selected literature identifies five general areas in which these transformations can occur. The potential sources of change for which DR planners should account are summarized in Table 8 (see below):

Source of change	Description
Technology	Snedaker (2007) summarizes the changes that can occur to the technology that comprise time-critical IT systems as including hardware or software upgrades, reconfigurations, and the retirement of aging components (p. 394).
Corporate	Gregory (2008) cautions that structural changes at the corporate level, such as those that result from mergers and acquisitions, can require significant changes to a DR plan due to the convergence of previously disparate IT systems (p. 243).
Operations	As reported by Snedaker (2007), changes within a business, such as reorganization, expansion, new departments, or new facilities can all affect the procedures outlined within a DR plan (p. 395).
Personnel	The loss of technology experts and experienced members of a disaster response team, warns Gondek (2002), poses "one of the greatest risks" to DR planning due to those individuals' implicit knowledge of the company's IT systems and recovery processes (p. 18).
External	DR plans are vulnerable to changes outside of a business as well as within, such those that affect the legal, regulatory, or compliance landscape (Snedaker, 2007, p. 396). Gregory (2008) notes that changes in the competitive marketplace, such as an increase in outsourcing, may also require revisions to a DR plan (p. 247).

Table 8: Potential sources of change that can affect a DR plan

Gregory (2008) notes that, depending on the organization, some of the changes outlined in Table 8 (see above) will only require a revision to specific recovery procedures while others may necessitate that the entire BIA process be revisited (p. 249). Snedaker (2008) adds that, although there are many potential sources for change, implementing processes to monitor each area can ease DR plan maintenance activities (p. 397). The specific monitoring procedures selected by each organization should be identified as a part of the change management strategy, which is described below.

Selecting the change management strategy. Snedaker (2007) characterizes two distinct strategies for managing changes to a DR plan: (1) monitoring business processes continually and

responding promptly when changes are needed, and (2) scheduling periodic reviews of changes to business processes (p. 396). Toigo (2003) notes that the need for changes to a DR plan can also be signaled through plan testing and validations processes, which are described in Stage 3 (see above) (p. 427). However, adds Toigo (2003), defining an explicit change management strategy is the "preferred" method to identify and respond to needed changes (p. 427).

According to Toigo (2003), DR planners utilizing a continuous monitoring strategy should evaluate business processes and the supporting IT infrastructure to "identify elements that are likely to change over time" (p. 428). Triggering events should be defined and embedded into the business processes that are likely to change, so that when changes occur, "they can be quickly assessed for their potential impact on the DR plan" (Snedaker, 2007, p. 397). Changes that will have no impact can be ignored, advises Snedaker (2003), but those that will affect a DR plan should require the submission of a change notification form to which the DR planning team can respond as-needed (p. 397).

Like the monitoring strategy, the periodic evaluation approach requires that a change notification process be integrated into any business activities that could affect a DR plan (Snedaker, 2007, p. 398). However, rather than keeping DR team members on call to evaluate and respond promptly to changes, a member of the DR planning team is assigned to review change notifications on scheduled intervals (Snedaker, 2007, p. 398). While this approach can delay the response to changes, having revisions evaluated collectively can improve the planning team's efficiency when amending a DR plan (Snedaker, 2007, p. 398).

Maintaining the planning documentation. At the conclusion of a DR planning initiative, multiple documents will have been created that collectively comprise an organization's DR plan

(Snedaker, 2007, p. 256). Wells et al. (2007) cautions that organizations should implement change control procedures to protect these documents by requiring changes to be approved by a designated change control board or committee (p. 236). Once changes are approved, Snedaker (2007) advises, the following details should accompany all changes to DR planning documentation: (a) reason for the change, (b) description of the change, (c) author of the change, (d) version number, and (e) who approved the change (Snedaker, 2007, p. 258). Once a document has been changed, Snedaker (2007) adds, another member of the DR planning team should review the change, and the reviewer's name should also be documented (p. 258).

The formal change management process should not incorporate all of the documents associated with DR planning. As noted in the *Defining and documenting specific recovery processes* section (see above), the maintenance of detailed recovery procedures for each time-critical IT system should be performed independently by the members of the disaster response team who would perform those activities in the wake of a disaster (Bradbury, 2008, p. 16).

Conclusions

This literature review is designed to assist the members of disaster recovery planning teams in the development of strategies to recover time-critical IT systems after a disaster. The study presents information that is authored or endorsed by experts and academics in the DR planning field. This information is analyzed using a formal conceptual analysis process to ensure that the selected literature discusses DR planning key elements in a context that allows the information to be appropriately generalized for this study's audience (Busch et al., 2005).

Through a synthesis of information that is drawn from a wide variety of credible sources, this literature review presents specific key elements and supporting best practices that comprise an effective DR plan for time-critical business IT systems. Prior to beginning a DR planning effort, Gregory (2008) suggests that businesses should "imagine what effects a disaster would have" on the organization (p. 30). In the *Importance of Disaster Recovery Planning* section that follows, key arguments in support of DR planning are described to underscore the need for businesses to develop DR plans. Once organizations have decided to develop a DR plan, a team should be organized and tasked with conducting a formal DR planning project (Toigo, 2003, p. 28). The *Disaster Recovery Planning Stages* section below summarizes the major themes that the selected literature indicates should be included in a DR planning project. Although DR planning to protect time-critical IT systems is reportedly vital, Snedaker (2007) suggests that DR planning alone is not enough to certify that an organization can recover from a disaster (p. 4). The *Achieving Comprehensive Disaster Preparedness* section below describes the relatively limited function that DR plays within the larger context of business continuity planning. This suggests

that organizations should employ additional risk management strategies to guarantee comprehensive disaster preparedness.

Importance of Disaster Recovery Planning

Many of the authors cited within this literature review emphasize the importance of DR planning to business survival. As Decker (2005) explains, the ability for a business to successfully emerge from a disaster lies more in what that business did to prepare for the event than in how it reacted after the disaster took place (p. 44). As organizations become increasingly dependent on technology (Bhatt & Grover, 2005, p. 255), disaster preparation for many businesses now necessitates the development of an explicit strategy to ensure that temporary replacements for damaged time-critical IT systems can be rapidly deployed (Lesser, 2004, p. 70). Furthermore, adds Toigo (2003), IT staff members are bound by an "ethical mandate," sometimes stated in an explicit service level agreement with other departments, to guarantee the reliability of IT systems (p. 8).

A common thread that is reiterated throughout the selected literature is that businesses without effective DR plans in place are exposed to significant risks. Those risks can include (a) small incidents such as a fire or flood in an IT server room, (b) large events such as a major earthquake or hurricane (Snedaker, 2007, p. 33), or (c) an extended loss of services such as electricity and Internet connectivity (Gregory, 2008, p. 67). Spencer & Johnston (2003) warn that the cumulative loss from seemingly small disasters can exceed the potential damage produced by a large event (p. 99). Relatively small disasters can interrupt business operations for days, which is potentially devastating since, according to Gregory (2008), 40 percent of companies that shut down for three or more days fail within 36 months (p. 11).

As indicated in the *Significance* section (see above), the risks posed by disasters are underscored by the likelihood that a disaster will strike and the potential impact of such a disaster. According to Decker (2005), disasters afflict over 90 percent of businesses at some point in time and nearly half of those affected cease operations within five years (p. 44). As Toigo (2003) notes, unprepared businesses that do recover from a disaster can face substantial financial losses (p. 48). Regardless of whether or not organizations are fully aware of the risks with which they are faced, Chisholm (2008) warns that 60 percent of North American businesses have not developed a DR plan.

Disaster Recovery Planning Stages

Resources for this literature review are selected and analyzed with the objective of answering the following research question: "What are the most important elements of an effective disaster recovery plan for information technology systems?" The selected literature presents multiple themes that, when synthesized and organized sequentially, sufficiently satisfy the guiding research question.

The DR planning key elements and supporting best practices that are identified within this study are organized into a five-stage process. This process can be used to guide the efforts of IT professionals, as well as other individuals who are involved in DR planning, in the identification of risks that face an organization's time-critical IT systems and the development of an explicit strategy to address those risks. Table 9 (see below) summarizes the five DR planning stages (described fully in the previous section of this document) and describes the major tasks that the literature indicates should be conducted within each stage:

DR planning stage	Major tasks to be conducted by the business
Stage 1: Project Initiation	Businesses must establish the need for disaster planning and define a project plan to guide the development efforts (Clas, 2008, p. 47). An effective initiation process helps to assure the success of the resulting DR plan (Snedaker, 2007, p. 33). The major tasks included in the initiation stage are as follows: • Securing management support • Organizing the planning project team • Establishing the project management process • Obtaining the required resources • Developing initial project objectives
Stage 2: Conducting a Business Impact Analysis	A Business Impact Analysis (BIA) evaluates an organization's IT systems to determine which systems should be included in a DR plan (Gregory, 2008, p. 51), and in what order the selected systems should be recovered (Bradbury, 2008, p. 16). A BIA involves these tasks: • Gathering information • Identifying the time-critical IT systems • Performing a risk assessment • Prioritizing the recovery efforts
Stage 3: Developing a DR Plan	Based on the information revealed in the BIA process, this stage requires the identification and documentation of specific procedures to be invoke in the event of a disaster (Snedaker, 2007, p. 294). The following tasks are required to develop an effective DR plan: • Selecting the risk management strategies • Defining disaster severity levels • Identifying activation triggers • Defining and documenting specific recovery processes • Selecting disaster response team members
Stage 4: Testing a DR Plan	Once a plan has been developed, it must be tested to ensure that it can accomplish the recovery objectives (Rothstein, 2007, p. 10) that are defined in the BIA for each time-critical IT system. If problems are revealed in this stage, the DR plan must be revised and the test repeated (Gregory, 2008, p. 218). Major testing tasks include: • Developing a test strategy

DR planning stage	Major tasks to be conducted by the business
	• Training the recovery staff • Conducing the test procedures • Establishing the test frequency
Stage 5: Maintaining a DR Plan	During the maintenance stage, processes are established to guarantee that DR plans are reliably updated to reflect the current requirements of continuously changing business processes (Toigo, 2003, p. 424). The tasks required to maintain a DR plan are as follows: • Identifying potential sources of change • Selecting the change management strategy • Maintaining the planning documentation

Table 9: Summary of the five DR planning stages

As Wells et al. (2007) indicates, there exist many strategies for developing a DR plan, so the extent to which the process outlined above is applicable to each business depends entirely on that business' unique requirements and expectations (p. 28). Furthermore, although this literature review is informed by best practices, "no best practice remains best for very long" (*Best practice*, n.d.), so that readers are encouraged to conduct additional research to evaluate the current relevancy of the information provided.

Achieving Comprehensive Disaster Preparedness

As Bradbury (2008) explains, developing a DR plan to make certain that time-critical IT systems are promptly restored after a disaster is a crucial activity since most businesses could not function without key technology (p. 14). However, organizations should not limit their disaster planning to IT systems alone (Cerni, 2006). For example, successfully activating a hot site to restore critical IT functions is not likely to improve a business' survivability if there are no staff members available to operate those systems. Wells et al. (2007) advises that DR planning should be combined with additional preparations to form a comprehensive BC plan (p. 19).

According to Snedaker (2007), the purpose of BC planning is to ensure that businesses can maintain continuous operations "before, during, and after disasters and disruptive events" (p. 3). Clas (2008) suggests a broad range of factors that should be addressed within a BC plan, including the availability of IT systems, personnel, facilities, and the financing needed by an organization to fund ongoing operations (p. 46). BC plans extend far beyond immediate disaster response activities to address long-term issues such as guaranteeing that an organization's supply chain remains intact (Wells et al., 2007, p. 19).

Selected literature in both areas of DR and BC planning indicates that the obstacles preventing organizations from developing a comprehensive BC plan are largely the same as those that must be overcome for DR planning to commence (see *Stage 1: Project Initiation* above). Thus it is likely that individuals who have accessed this literature review to guide the development of a DR plan may have already established the foundation needed to justify a BC planning initiative. Cerni (2006) urges that DR planners build upon this foundation by incorporating DR plans into a "greater enterprise BC plan," which guarantees that "organizations can protect corporate viability and ensure a continuity of operations to customers, partners, and investors" (para. 14).

Although BC efforts should compliment DR planning to achieve comprehensive disaster preparedness, organizations should develop DR plans regardless of whether or not a BC planning effort has been approved. DR planning can dramatically increase an organization's ability to recover from a wide range of potential disasters (Snedaker, 2007, p. 4). In addition to enabling effective disaster recovery, DR planning activities such as the BIA process described in Stage 2 (see above) can reveal potential improvements to processes or technology that result in fewer

disruptions and higher quality services (Gregory, 2008, p. 13). As Gregory (2008) indicates, guaranteeing that critical services will withstand a disaster while potentially improving technology and processes can provide significant competitive advantage for an organization (p. 338). Strengthening the ability to surpass competitors will further ensure an organization's long-term viability, regardless of whether or not disaster strikes.

References

Abstract. (n.d.). *BusinessDictionary.com*. Retrieved December 1, 2008, from: http://www.businessdictionary.com/definition/abstract.html

Alonso, F., Boucher, J., & Colson, R. H. (2001, November). Business continuity plans for disaster response [Electronic version]. *CPA Journal*, 60-60.

Barrier, M. (2001). Preparing for the worst [Electronic version]. *Internal Auditor*, 57-61.

Best practice. (n.d.). *BusinessDictionary.com*. Retrieved November 22, 2008, from: http://www.businessdictionary.com/definition/best-practice.html

Bhatt, G. D., & Grover, V. (2005). Types of information technology capabilities and their role in competitive advantage: an empirical study [Electronic version]. *Journal of Management Information Systems*, 253 - 277.

Bradbury, C. (2008). Disaster! [Electronic version]. *British Journal of Administrative Management*, 14-16.

Busch, C. De Maret, P. S., Flynn, T. Kellum, R., Le, S., Meyers, B., Saunders, M., White, R., and Palmquist, M. (2005). *A state of the art review*. Writing@CSU. Colorado State University Department of English. Retrieved December 8, 2008, from http://writing.colostate.edu/guides/documents/review_essay/com2a1.cfm

Busch, C. De Maret, P. S., Flynn, T. Kellum, R., Le, S., Meyers, B., Saunders, M., White, R., and Palmquist, M. (2005). *Content analysis*. Writing@CSU. Colorado State University Department of English. Retrieved November 26, 2008 from http://writing.colostate.edu/guides/research/content/

Busch, C. De Maret, P. S., Flynn, T. Kellum, R., Le, S., Meyers, B., Saunders, M., White, R., and Palmquist, M. (2005). *Methods of conceptual analysis*. Writing@CSU. Colorado State University Department of English. Retrieved December 8, 2008, from http://writing.colostate.edu/guides/research/content/pop3a.cfm

Caramia, M., & Felici, G. (2006). Mining relevant information on the Web: a clique-based approach [Electronic version]. *International Journal of Production Research*, 2771-2787.

Case study. (n.d.). *BusinessDictionary.com*. Retrieved November 22, 2008, from: http://www.businessdictionary.com/definition/case-study.html

Cerni, L. (2006). *Building a comprehensive disaster recovery plan*. Retrieved November 16, 2008, from Disaster Recovery Journal: http://www.drj.com/index.php?option=com_content&task=view&id=888&Itemid=429

Chernicoff, D. (2007, February 1). Disaster-preparedness checklist [Electronic version]. *Windows IT Pro Magazine*, pp. 49-53.

Chisholm, P. (2008, July). Disaster recovery planning is business-critical [Electronic version]. *CPA Journal*, 11-11.

Clas, E. (2008, September). Business continuity plans [Electronic version]. *Professional Safety*, 45-48.

Conz, N. (2008, January 1). Preparing for the worst [Electronic version]. *Insurance & Technology*, pp. 30-36.

Data. (2003, October 28). *Webopedia.com*. Retrieved January 17, 2009, from: http://www.webopedia.com/TERM/D/data.html

De Tura, N., Reilly, S. M., Narasimhan, S., & Yin, Z. J. (2004). Disaster recovery preparedness through continuous process optimization [Electronic version]. *Bell Labs Technical Journal*, 147-162.

Decker, A. (2005, January). Disaster recovery: what it means to be prepared [Electronic version]. *DM Review*, 44-46.

Drummond, S. (2008, February 15). Business continuity gets over IT [Electronic version]. *Lawyers Weekly*, pp. 14-15.

Gondek, R. (2002). When more of the same isn't better [Electronic version]. *Journal of Business Strategy*, 16-18.

Gregory, P. H. (2008). *IT disaster recovery planning for dummies.* Hoboken: Wiley Publishing, Inc.

Guide for developing a disaster plan. (2006, August 22). *University of Missouri*. Retrieved November 11, 2008, from: http://www.umsystem.edu/ums/departments/fa/management/records/disaster/guide/

Hardware. (n.d.). *BusinessDictionary.com*. Retrieved January 17, 2009, from: http://www.businessdictionary.com/definition/hardware.html

Hayes, J. (2005). Reaping the whirlwind [Electronic version]. *IEE Review*, 29-29.

Heffes, E. M. (2002). Best practices... by definition [Electronic version]. *Financial Executive*, 44-45.

Hlavacek, D. M., Madsen, K. A., & Reimer, R. M. (2004). A vendor and service provider partnership for preparing to manage disaster recovery [Electronic version]. *Bell Labs Technical Journal,* 173-180.

Jargon. (n.d.). *Merriam-Webster's Online Dictionary*. Retrieved December 9, 2008, from: http://www.merriam-webster.com/dictionary/jargon

Jrad, A., Morawski, T., & Spergel, L. (2004). A model for quantifying business continuity preparedness risks for telecommunications networks [Electronic version]. *Bell Labs Technical Journal*, 107-123.

Leedy, P. D., & Ormrod, J. E. (2005). *Practical Research.* Upper Saddle River, NJ: Pearson Education.

Lesser, A. (2004). Pre-testing DR plans to avoid business interruption [Electronic version]. *Disaster Recovery Journal*, 70-72.

Literature review. (2007). *University of North Carolina*. Retrieved November 25, 2008, from: http://www.unc.edu/depts/wcweb/handouts/literature_review.html

North, E., North, J., & Benade, S. (2004). Information management and enterprise architecture planning - a juxtaposition [Electronic version]. *Problems & Perspectives in Management*, 166-179.

Obenzinger, H. (2005). *What can a literature review do for me?* Retrieved December 9, 2008, from Stanford University: http://ual.stanford.edu/pdf/uar_literaturereviewhandout.pdf

OneSearch. (n.d.). *UO Libraries*. Retrieved November 30, 2008, from: http://libweb.uoregon.edu/dc/onesearch/gateway.php?func=meta-1

PDF. (n.d.). *Webopedia.com*. Retrieved December 1, 2008, from: http://www.webopedia.com/TERM/P/PDF.html

Peer review. (n.d.). *BusinessDictionary.com*. Retrieved November 30, 2008, from: http://www.businessdictionary.com/definition/peer-review.html

Risk mitigation. (n.d.). *BusinessDictionary.com*. Retrieved January 18, 2009, from: http://www.businessdictionary.com/definition/risk-mitigation.html

Risk transfer. (n.d.). *BusinessDictionary.com*. Retrieved January 18, 2009, from: http://www.businessdictionary.com/definition/risk-transfer.html

Rothstein, P. J. (2007). *Disaster recovery testing.* Brookfield: Rothstein Associates.

Ryan, J. J., & Ryan, D. J. (2005, February). Proportional hazards in information security [Electronic version]. *Risk Analysis: An International Journal*, 141-149.

Smith, T. D. (2008, September 4). *Critical evaluation of information sources*. Retrieved November 8, 2008, from UO Libraries: http://libweb.uoregon.edu/guides/findarticles/credibility.html

Smith, T. D. (2006, September 22). *Scholarly or popular?* Retrieved November 8, 2008, from UO Libraries: http://libweb.uoregon.edu/guides/findarticles/distinguish.html

Snedaker, S. (2007). *Business continuity & disaster recovery for IT professionals*. Burlington: Syngress Publishing, Inc.

Software. (n.d.). *BusinessDictionary.com*. Retrieved January 17, 2009, from: http://www.businessdictionary.com/definition/software.html

Spencer, R. H. & Johnston, R. P. (2003). *Technology best practices.* Hoboken: John Wiley & Sons, Inc.

Stacks, G., & Karper, E. (2008, September 3). *Annotated bibliographies*. Retrieved December 9, 2008, from The Owl at Purdue: http://owl.english.purdue.edu/owl/resource/614/01/

Tainter, M. (2008). *Use ITIL to enhance your disaster recovery capability*. Retrieved December 13, 2008, from ITSM Watch: http://www.itsmwatch.com/itil/article.php/11700_3725506_2

Teuten, P. C. (2005, September). The top ten mistakes in risk management [Electronic version]. *Financial Executive*, 45-45.

Toigo, J. W. (2003). *Disaster recovery planning: preparing for the unthinkable.* Upper Saddle River: Prentice Hall PTR.

Weiner, S. (2001). Managing effective disaster recovery [Electronic version]. *CPA Journal*, 22-26.

Wells, A., Walker, C., & Walker, T. (2007). *Disaster recovery principles and practices.* Upper Saddle River: Pearson Prentice Hall.

What is ITIL. (n.d.) *ITIL.org*. Retrieved December 13, 2008, from: http://www.itil.org/en/