Global Information Assurance Certification Paper

Elements of a Disaster Recovery Plan

Tom Taylor

October 14, 2003

GIAC Security Essentials Certification Practical Assignment

Version 1.4b

Abstract

After the destruction of the World Trade Center on September 11, 2001, many corporations began focusing on a disaster recovery for the very first time. Some corporations implemented a disaster recovery plan in a timely manner and some corporations are still struggling with it.[1] This paper is intended to help those struggling corporations jump start their disaster recovery plans for their Information Technology department. The elements of the disaster recovery plan presented in this paper are: table of contents, general description, emergency procedures, risk analysis and critical applications, computer room procedures, recovery site procedures, recovery teams, computer room information, staff telephone list and call assignments, support agreements, disaster recovery log, plan maintenance procedures, and appendix. Rather than focus on theory, this paper instead presents detailed example wording of each element using the fictitious WidgetTech Corporation and it should stimulate your thoughts toward writing a practical disaster recovery plan for your corporation.

Table of Contents

The first element of a disaster recovery plan is the table of contents. When in the midst of a disaster, a simple and easy to understand table of contents can be a lifesaver. Without a doubt, the most important aspect of the table of contents in a time of crisis are the page numbers of each section of the disaster recovery plan. Also, a table of contents should provide enough details to the reader to help him find the information needed quickly without having to thumb through the plan. The following is an example of a table of contents.

TABLE OF CONTENTS

General Description

In the General Description element of the Disaster Recovery plan are three sub elements, which are Introduction, Management Overview and Responsibilities, and Plan Definitions. This section explains the purpose and lays the groundwork for the entire Disaster Recovery plan. Below are examples of each section for the fictitious WidgetTech Corportion.

Introduction

The WidgetTech Corporation is committed to recovery of critical applications on the company's computer network. These critical applications – payroll, web e-commerce, accounting, electronic mail (e-mail), file server, word processing – are necessary to keep the WidgetTech Corporation functioning at a minimal level during an emergency or disaster situation. (See the Risk Analysis and Critical Applications Section) This document contains a plan and other information required (1) to recover these applications rapidly in the event of a disaster, (2) to test the plan, and (3) to maintain the plan.

Management Overview and Responsibilities

The development, preparation, testing, and implementation of the plan is the responsibility of the Emergency Management Team. The Emergency Management Team will meet annually to review and modify the plan, as well as review results of plan tests.

Definitions[2]

"Disaster" is a sudden, unplanned calamitous event that creates an inability of an organization's parts to provide critical business functions for some predetermined period of time and that results in great loss or damage. Because many disasters are of limited duration, limited scope, and limited severity, we have developed a disaster recovery plan for the WidgetTech Corporation to recover any or all of its critical applications in any situation up to a "key disaster scenario" as outlined below.

"Critical applications" are those information technology applications that are necessary for the WidgetTech Corporation to survive and carry out its operations. As determined by risk analysis, the WidgetTech Corporation's critical applications are (1) payroll, (2) web e-commerce, (3) accounting, (4) electronic mail, (5) file server and (6) word processing. All other applications on the company's computer network are not critical and will not receive significant consideration in this plan.

"Risk" is any situation or condition that will bring about a disaster for the

WidgetTech Corporation's information system.

"Recovery" is the re-establishment of an information technology application or system to a pre-defined level of operation. In only a few instances will this recovery be for 100% of an application's service within a short period of time. For the WidgetTech Corporation, the only application that requires 100% of functionality within one day is the payroll system. As determined in the risk analysis and recovery section below, all other applications – including the other critical applications – will experience significant service degradation within the first week following a disaster.

"Restoration" is the return to "normal" operation in the new, permanent facilities for the information and telecommunication system. It is important to keep in mind that restoration after a major regional disaster could take several months to accomplish. It is equally important to note that a "normal" situation might take years to achieve and the WidgetTech Corporation will never recover all of the costs incurred in planning for or achieving restoration.

Emergency Procedures

In the Emergency Procedures element of the Disaster Recovery plan are three sub elements, which are Emergency Management Team, Emergency Outside Telephone Numbers, and General Emergency Procedures. This section details the individuals who can declare a disaster, who they should contact, and the procedures to follow. Below are examples of each section for the fictitious WidgetTech Corportion.

Emergency Management Team

The emergency management team is made up of the following individuals:

Information Technology Director
Information Technology Network Manager
Information Technology Applications Manager
Information Technology Security Officer
Accounting Director
Sales Director
Facilities Security Chief Officer

Note: The names and contact information for the above are in the Appendix.

The emergency management team will be the group that issues a declaration of a disaster, and the same group will determine when the

recovery has been completed and restoration of "normal" operation is to begin.

Emergency Outside Telephone Numbers

The following telephone numbers should be used for emergency service:

General Emergency	911
State Police	123-456-7890
State Bureau of Investigation	123-456-7891
State Emergency Management	123-456-7892
XYZ Insurance	123-456-7893

The telephone numbers to obtain information and equipment from primary suppliers are in the appendix.

General Emergency Procedures

Along with the consideration of recovery of critical operations, a primary consideration is for the safety of the staff of the WidgetTech Corporation. The following procedures should be used in the event of a disaster.

Fire/Other Building Evacuation

In the event of a fire alarm, the staff should evacuate the buildings. Until clear evidence that a fire exists, a member of the emergency management team should remain in the computer room in and be ready to do a normal shutdown of the computers. When clear evidence exists that there is a fire in the building that will threaten the loss of information systems function or a loss of data, emergency management staff should commence a controlled shutdown of all computers in the computer room and join the building evacuation.

Bomb Threats

In the event of a bomb threat, the staff should evacuate the buildings. Until clear evidence that the bomb threat is against the computer center, a member of the emergency management team should remain in the computer room and be ready to do a normal shutdown of the computers. When clear evidence exists that the bomb threat is against the computer facilities and could result in the loss of the information systems function or a loss of data, emergency management staff should start a controlled shutdown of

all computers in the computer room and join the building evacuation.

Severe Weather Warning or Evacuation

In the event of a severe weather warning that requires general building evacuation or relocation to central, safe portions of the buildings, the staff should evacuate the buildings. Until clear evidence that the weather condition poses an immediate danger to safety in the building, a member of the emergency management team should remain in the computer room and be ready to do a normal shutdown of the computers. When clear evidence exists that the severe weather situation could result in the loss of the information systems function or a loss of data, emergency management staff should start a controlled shutdown of all computers in the computer room and join the building evacuation or temporary relocation.

Riots/Civil Disorders

In the event of civil disorder, members of the emergency management team should remain in the computer facility and depend upon assistance from the WidgetTech Corporation Police and other police officials. If ordered to leave by the police, emergency management staff should complete a controlled shutdown of all computers in the computer room prior to leaving.

Risk Analysis and Critical Applications

In the Risk Analysis[3] and Critical Applications element of the Disaster Recovery plan, you should do an analysis of your corporation's critical applications.[4] You never know when the CEO or CFO may pick up the Disaster Recovery plan and read it. As a result, this section should be straightforward and to the point. So, before committing the time and money required to develop and test a disaster recovery plan, it is important to determine those situations that pose a risk to the information systems operations of any corporation.[5] **Table 1** contains a list of the various threats that would trigger these risks[6] and create a potential or real disaster for the WidgetTech Corporation. By summing the "X" marks in each column, it is clear that the primary threats that create major disruption risks for the WidgetTech Corporation are (1) fires, (2) earthquakes, (3) tornadoes, and (4) hurricanes. However, I should point out that not all types of natural disasters are should in the examples below, such as earthquakes, mudslides, wildfires, etc. When doing your risk analysis for your corporation, you need to list the type of disasters that are prevalent in the area.

Below is a sample risk analysis matrix for the WidgetTech Corporation.

TABLE 1
WIDGETTECH CORPORATION
INFORMATION TECHNOLOGY DIVISION
RISK ANALYSIS MATRIX

THREAT / **RISK**	Fire	Earth-quake	Tornado	Hurricane	Sabotage	Thunder-storm	Civil Disturb.	Catastrophic Explosion	Nuclear Accident	Equip. Failure
Power Outage	X	X	X	X	X	X	X	X	X	X
Building Destruction	X	X	X	X	_	_	_	X	_	_
Internal Fire Destruction	X	_	_	_	X	_	X	_	_	X
Telecommunications Network Outage	X	X	X	X	X	X	X	X	X	X
Lengthy Building Evacuations	X	X	X	X	_	_	_	X	X	_
Major Flood	_	_	_	X	_	_	_	_	_	_
Internal Water Destruction	X	X	X	X	X	X	_	_	_	X
Equipment Failure	X	X	X	X	X	_	X	X	_	X

By summing the "X" marks in each row, it is apparent that the greatest risks to the WidgetTech Corporation's information systems are (1) power outages, (2) telecommunications network outages, (3) internal water destruction, and (4) equipment failure.

The use of personal computers is growing slowly and steadily in the WidgetTech Corporation. While users view them as "personal" productivity tools, information systems professionals also must view them as "computers." They have with them the needs for security and disaster recovery that are attached normally to servers and large networks. Only the scale of the needs varies.

Table 2 contains an example of a security and disaster recovery risk analysis matrix for personal computers.

TABLE 2
WIDGETTECH CORPORATION
INFORMATION TECHNOLOGY DIVISION
PERSONAL COMPUTER SECURITY AND DISASTER RECOVERY RISK ANALYSIS MATRIX

THREAT	Fire	Employee Error	Tornado	Hurricane	Sabotage	Virus Attack	Civil Disturb.	Catastrophic Explosion	Nuclear Accident	Equip. or Software Failure
RISK TO PERSONAL COMPUTER USERS										
Loss of Data	X	X	X	X	X	X	X	X	_	X
Disclosure of Confidential Information	_	X	_	_	X	_	X	_	_	X
Destruction of Data	X	X	X	X	X	X	X	X	_	X
Loss of access to PCs for use and processing	X	X	X	X	X	X	X	X	X	X
Destruction of Computer Programs	X	X	X	X	X	X	X	X	_	X

The WidgetTech Corporation has taken substantial steps to control the likelihood of fire destruction in the building. An examination of the list points to the importance of the uninterruptible power supply, the diesel generator, and preventative maintenance in keeping the WidgetTech Corporation's information systems operational. Additional tests of the equipment, periodic checks for spare parts, and improved redundancy of data communications capabilities are needed to mitigate potential services interruptions from fire, weather, and equipment failure.

Table 3 contains the controls now in place to mitigate these risks.

TABLE 3
WIDGETTECH CORPORATION
INFORMATION TECHNOLOGY DIVISION
RISK CONTROLS AND MITIGATION FACTORS

THREAT	MITIGATION FACTOR
FIRE	Fire alarms; Standpipes; Halon System in Computer Room; Fire Extinguishers in sensitive network rooms; Security plan; Camera surveillance; Periodic police rounds; Automated environmental monitoring system.
EARTHQUAKE	Very low potential.
TORNADO	Weather warnings; Drills; UPS; Diesel generator; Automated environmental monitoring system.
HURRICANE	Weather warnings; Drills; Evacuation; UPS; Diesel generator; Automated environmental monitoring system.
SABOTAGE	WidgetTech Corporation Police; Security checks; Security plan, Motion detectors; Camera surveillance; Periodic police rounds; Restricted physical access; Employee awareness; Daily operations environmental system checklist; Automated environmental monitoring system.
THUNDERSTORM	Weather warnings; UPS; Diesel generator; Automated environmental monitoring system.
CIVIL DISTURBANCE	WidgetTech Corporation Police; Security checks; Security plan, Motion detectors; Camera surveillance; Restricted physical access Automated environmental monitoring system.
CATASTROPHIC EXPLOSION	Redundancy of most vital computer and network equipment; Computer Backup Tapes Offsite; Disaster Recovery Computer Site
NUCLEAR ACCIDENT	Power company warnings and emergency alert system. UPS; Diesel generator; Automated environmental monitoring system.
EQUIPMENT FAILURE	Preventive maintenance; Redundancy of most vital computer and network equipment; Spare parts inventory; Vendor maintenance contracts; Automated environmental monitoring system; Daily operations environmental system checklist; Periodic WidgetTech Corporation Police checks.

Table 4 contains the basic recovery alternatives in the event a risk becomes real and creates a disaster for the WidgetTech Corporation's information system. In the estimated cost columns of the table, you will see I have $0 (+labor) and TBD. When you do your corporation's version of the table, you will need to do the unenviable task of doing the calculations and entering them in the columns. As you can see in the table, payroll, web e-commerce, accounting, electronic mail, file server, and word processing are the critical applications for the WidgetTech Corporation to resume operation in the event a "key disaster scenario" develops.

TABLE 4
WIDGETTECH CORPORATION
INFORMATION TECHNOLOGY DIVISION
ACCEPTABLE RECOVERY STRATEGIES FOR APPLICATIONS

Application System	Priority	Maximum Accept-able Recovery Time	Most Probable Accept-Able Recovery Strategies	-----ESTIMATED Prepara-tion	COST------ In Use [Daily]
CRITICAL APPLICATIONS:					
Payroll	Highest	1 day	Recover to another server on network;	$0 (+labor)	$0 (+labor)
			Recover to disaster recovery site	TBD	TBD
Web E-commerce	High	1 day	Recover to another server on network	$0(+labor)	$0(+labor)
			Recover to disaster recovery site	TBD	TBD
Accounting	High	1 day	Recover to another server on network	$0(+labor)	$0(+labor)
			Recover to disaster recovery site	TBD	TBD
Electronic Mail	High	1 day	Recover to another server on network	$0(+labor)	$0(+labor)
			Recover to disaster recovery site	TBD	TBD
File Server	Medium	2 days	Recover to		

			another server on network	$0(+labor)	$0(+labor)
			Recover to disaster recovery site	TBD	TBD
Personal Computer Applications					
Word Processing (with File and Print capabilities)	Medium	2 days	Recover on existing and acquired P.C.s	$0 on existing P.C.s and $2000 per P.C. on new P.C.s	$0(+labor)

A sub element of this section is the Disaster Scenario.[7] Here you should present a "paper walk through" of a disaster. This section is in essence your "proof of concept" section for the disaster recovery plan. Below is example of this section using the fictitious WidgetTech Corporation:

> For purpose of developing this list of critical applications and the most probable recovery strategies for each, we assumed a **"key disaster scenario"** of the following:
>
> > ***"The WidgetTech Corporation has two more weeks left in the current fiscal year. A tornado touches down in the heart of city, destroying major parts of the Corporation's building."***
>
> While we can conjure up other calamities, we believe this key disaster scenario is realistic and believable. By planning to meet this key disaster scenario, we can meet in disasters of a lesser magnitude. Here are the activity phases that will occur in the event of a disaster. (The times listed are the maximum times allotted for the activities. However, in the event of an internal, on-site recovery to another server on the network, all of the tasks should be carried out in less time.)
>
> **Phase 1:** The Emergency Management Team reviews the situation and, upon recommendation of the Director of the Information Technology Division, declares a disaster. The declaration will be issued to corporation leadership, staff, police authorities, and vendors of critical hardware, software, and services.
>
> If the facilities of the WidgetTech Corporation building are intact, the first meeting will occur in this facility. If the facility is not intact, the first

meeting of the Emergency Management Team will occur at the XYZ Hotel at the corner of Main St. and First St. If that facility is not available, the Emergency Management Team will meet at the 123 Hotel in Anyclosecity. At its first meeting after the declaration, the Emergency Management Team will recommend procedures and sites for relocating non-information systems staff during the recovery phase. At its first meeting, the Emergency Management Team will determine all future meeting times and locations for the information technology staff.

Phase 2: The Emergency Management Team assesses the impact and severity of the disaster and selects from the acceptable recovery strategies for each of the critical applications—based on the estimated duration of the disaster condition and its results.

1 – 6 Hours After the Declaration

Assess the damages
- Establish a central location for decision-making
- Notify senior management in the WidgetTech Corporation of the disaster situation
- Determine if the recovery will be with internal resources or through use of the shell site
- Inform the recovery teams that have been affected of the situation and instruct them on the actions to be taken
- Notify the backup site(s) of the need, or lack of need, to use their facilities

Phase 3: The Emergency Management Team instructs the various Information Systems Division teams to implement their recovery strategies.

1 – 6 Hours After the Declaration
- Initiate transportation to the backup site
- Assemble recovery teams at the backup site
- Start movement of supplies and tapes

6 – 12 Hours After the Declaration
- Notify users who will assist in the recovery
- Establish hardware, software, and supply needs
- Order any necessary supplies and equipment
- Move off-site tapes and documentation to backup site

12 – 24 Hours After the Declaration
- Transportation system is working fully
- Establish operations at backup site
- Bring up the operating system if not on a "Hot" machine

- Test all backup equipment
- Restore disk files using backup tapes
- Restore and test the database(s)
- Begin testing to verify file integrity

24 Hours after Being Notified

- Salvage all usable material and documentation
- Stat recovering all critical systems to current status
- Review application recovery to determine status
- Establish processing schedule for operations
- Start processing schedule of operations
- Start processing critical applications

Phase 4: The Emergency Management Team reviews the situation daily to declare the end to the disaster situation and to begin restoration of "normal" operations.

Computer Room Procedures

In the Computer Room Procedures element of the Disaster Recovery plan are two sub elements, which are Power Down Procedures, and Obtaining Backup. This section details the emergency procedures related specifically to the computer room. Below are examples of each section for the fictitious WidgetTech Corporation:

Power Down Procedures

There are standard power down procedures for all equipment in the Computer Room in the building. If time does not permit, hit the emergency "power off" button by the door of the computer room on your way out. This step will be taken only by or at the direction of the Information Technology Director, Information Technology Network Manager, or Information Technology Applications Manager.

Obtaining Backup Files

The latest differential and full backup recovery tapes will be obtained at the following location:

ABC Tape Storage Inc.
123 Main St.
Anycity, Anystate 12345
123-456-7895

Ask for Sam Tape or Anthony Disk

If after hours, weekends, holidays, or no answer at 123-456-7895, please call the pager at 123-456-7896

Recovery Site Procedures

The Recovery Site Procedures element of the Disaster Recovery plan should address the actions that should be taken at the recovery site. Since your recovery site vendor may change from time to time and/or the contract itself, I recommend this section reference an Appendix section where changes can be made easier. Below is an example of this section for the fictitious WidgetTech Corporation:

> The WidgetTech Corporation has entered into a formal disaster recovery site arrangement with 123 Recovery Services. The agreement with 123 Recovery Services is contained in the Appendix. Procedures for recovering any or all of the critical applications to the disaster recovery site are contained in Appendix.

Recovery Teams

In the Recovery Teams[8] element of the Disaster Recovery plan are twelve sub elements, which are Emergency Management Team, Data Center Operations Team, Server Operating System Team, Communications Team, Web E-commerce Team, Database Team, E-mail Team, File Server Team, Personal Computer Team, ISF (Insurance, Salvage, and Facilities) Restoration Team, Special Projects Team, and Internal Audit Team. This section should detail the teams responsible for specific areas of recovery. Below are examples of each section for the fictitious WidgetTech Corportion

> **Emergency Management Team**
>
> The emergency management team is made up of the following individuals:
>
> Information Technology Director
> Information Technology Network Manager
> Information Technology Applications Manager
> Information Technology Security Officer
> Accounting Director
> Sales Director
> Facilities Security Chief Officer
>
> Note: The names and contact information for the above are in the Appendix.

The emergency management team will be the group that issues a declaration of a disaster, and the same group will determine when the recovery has been completed and restoration of "normal" operation is to begin.

Data Center Operations Team

The data center operations recovery team will be responsible for the following recovery operations on-site and at any off-site center that might be used during recovery operations.

(1) Computer Operations
(2) Facility Preparation
(3) Replacement Hardware
(4) Disaster Recovery Site Preparation
(5) Data Processing Supplies
(6) Offsite Storage Procedures

The names of the members of the data center operations recovery team are in the Appendix.

Server Operating System Team

The server operating system team will be responsible for setting up the operating system and directory services on all servers. The names of the members of the server operating system team are in the Appendix.

Communications Team

The communications team will be responsible for setting up all data communications operations during recovery and restoration operations. The names of the members of the communications team are in the Appendix.

Web E-commerce Team

The Web E-commerce team will be responsible for recovering the Web E-commerce application. The names of the members of the Web E-commerce team are in the Appendix.

Database Team

The database disaster team will be responsible for recovering critical database applications, with particular emphasis on payroll. Following recovery of payroll, the team will recover Accounting. This team will spend no time recovering any other database applications until after

payroll and Accounting are fully operational. The names of the members of the database team are in the Appendix.

Electronic Mail Team

The electronic mail team will be responsible for recovering the electronic mail system. The names of the members of the electronic mail team are in the Appendix.

File Server Team

The file server team will be responsible for recovering the file server. The names of the members of the file server team are in the Appendix.

Personal Computer Team

The personal computer team will be responsible for installing and configuring new personal computers with needed applications (word processing, electronic mail client, etc.). The names of the members of the personal computer team are in the Appendix.

Insurance, Salvage, and Facilities (ISF) Restoration Team

The ISF restoration team will be responsible for coordinating all work with the Department of Insurance and the vendors for preparing the restoration site. The names of the members of the ISF restoration team are in the Appendix. Documents related to the insurance coverage for the WidgetTech Corporation's information systems are in the Appendix.

Special Projects Team

The special projects team will be responsible for the following:

(1) Administrative and Office Support;
(2) Transportation; and
(3) Purchasing and Supplies.

The names of the members of the special projects team are in Appendix.

Internal Audit Team

The internal audit team will review and test annually the disaster recovery plan for critical applications. The names of the members of the internal audit team are in Appendix.

Computer Room Information

In the Computer Room Information element of the Disaster Recovery plan, you should have additional information about the computer room that may be of use during a disaster. Depending on your environment, you could also name this section Data Center Information. Below is an example of this section for the fictitious WidgetTech Corporation. In the example below, you will notice that the Appendix is referenced extensively for flexibility in updating the information.

Computer Room and Tape Library Layout

The appendix contains the floor layouts for the computer room in the building.

Power Requirements, Cable Diagrams, and Plug Connectors

The appendix contains the electrical layout for the computer facility in the building. Because the personal computers required standard building power, no separate layout is included for personal computer locations. However, the emergency management team might purchase additional power condition and surge protection for these computers where needed.

Air Conditioning, Fire Protection, and Security

The appendix contains the air conditioning, fire protection, and security layout for the computer room in the building.

Computer Room and Network Equipment Inventory

The appendix contains the computer equipment inventory for all computers and major telecommunications equipment in the computer room in the building. The inventory also includes the network equipment located throughout the building.

System Software Licenses

The appendix contains a copy of the most recently issued software licenses.

Computer Systems Documentation

In Lieu of current copies of the system and utility software Manuals, the most recently retired versions of software manuals are stored at the tape backup site.

Staff Telephone List and Call Assignments

In this element of the Disaster Recovery plan, you should explain in detail "who should call who" in the event of a disaster in order to eliminate confusion. Below is an example of this section for the fictitious WidgetTech Corporation:

> In the event of a disaster, the following people will be responsible for making telephone calls to staff and vendors:
>
> The Information Technology Director contacts everyone on the Emergency Management Team (see the Appendix for the members of the team). In this call, the Information Technology Director will notify everyone of the location to which the recovery teams should proceed for recovery operations. If possible, this location will be the offices of the WidgetTech Corporation. If these offices are not available, the next location in line will be the XYZ Hotel at the corner of Main St. and First St. The third location in line will be the 123 Hotel in Anyclosecity. The fourth backup location will be the disaster recovery site.
>
> Next, the Information Technology Director contacts the Information Technology Client Services Manager to advise him/her of the disaster. After the call from the Information Technology Director, each of the Information Technology Managers (Applications, Client Services, and Network) calls everyone in the their respective group to advise them of the disaster and the forthcoming steps to be taken. Finally, the Information Technology Director, the Information Technology Network Manager, and the Information Technology Applications Manager will be responsible for all initial calls to vendors that need to be aware that a disaster has occurred.

With regard to the staff telephone numbers, I recommend for flexibility keeping the information in the Appendix so it can be easily updated. You will need this flexibility as people come and go in your corporation.

External Support Agreements

In the External Support Agreements element of the Disaster Recovery plan, you should address support agreements your corporation may have with third party vendors. The content of the section will vary from corporation to corporation. Below is an example of this section for the fictitious WidgetTech Corporation:

> The WidgetTech Corporation has no external support agreements apart from its regular maintenance agreements that will bear on its ability to

recover critical applications from disasters. See the Appendix for the maintenance agreements.

Disaster Recovery Log

In the Disaster Recovery Log element of the Disaster Recovery plan, you should discuss the use of logs during tests[9] and actual disasters (if time permits) to record actions taken, problems, and ideas.

Plan Maintenance Procedures

In the Plan Maintenance Procedures element of the Disaster Recovery plan, you should detail how the plan will be maintained. A Disaster Recovery plan is a "living document" that requires almost constant updating, especially in the Appendix section. Below is an example of this section for the fictitious WidgetTech Corporation:

> This plan will be maintained under the direction of the Information Technology Security Officer. The primary persons responsible for maintaining the currency and accuracy of the plan will be the Information Technology Network Manager, the Information Technology Applications Manager, and the Information Technology Business Analyst. The plan will be reviewed and updated formally by these four people, along with the Information Technology Division Director, every six months. It will receive modifications as necessary between the meetings.

Appendix

In the Appendix element of the Disaster Recovery plan, you should arrange it so the information contained in it is easily updated. Due to the various types of information kept in the Appendix, the Appendix needs to be carefully organized and each section numbered. The contents of the Appendix should be listed in the Table of Contents of the Disaster Recovery plan.

References:

- [1] Melissa Solomon (June 21, 2002). Disaster recovery after Sept. 11: Lessons learned. *Computer World*. Retrieved October 14, 2003, from http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,72192,00.html

- [2] Disaster Recovery Institute International. (n.d.). DRI International Business Continuity Glossary. Retrieved October 14, 2003, from http://www.drii.org/associations/1311/files/glossary.pdf

- [3] Security Risk Associates. (2001). The Benefits of Security Risk Analysis. Retrieved October 14, 2003 from http://www.eon-commerce.com/riskanalysis/benefits.htm

- [4] California Department of General Services. (February 2002). Identification of Critical Applications. Retrieved October 14, 2003, from http://sam.dgs.ca.gov/TOC/4800/4842.11.htm

- [5] Smithsonian Institution. (n.d.). Disaster Planning, Prevention and Recovery Manual for the Smithsonian Institution Archives. Retrieved October 14, 2003, from http://www.si.edu/archives/report/disaster/three.htm#threea

- [6] Library of Congress. (n.d.). Emergency Preparedness for Library of Congress Collections – Risk Assessment. Retrieved October 14, 2003, from http://lcweb.loc.gov/preserv/pub/seibert/risk.html

- [7] Disasterplan.com (n.d.). Getting Started: Disaster Recovery Planning Without Destroying Your Budget. Retrieved October 14, 2003 from http://www.disasterplan.com/yellowpages/Intro.html

- [8] University of Arkansas Computing Services. (October 10, 2002). Disaster Recovery Plan Disaster Recovery Teams. Retrieved October 14, 2003, from http://www.uark.edu/staff/drp/drpdr006.htm

- [9] Disasterrecoveryworld.com. (n.d.). Guidelines for Testing a Disaster Recovery Plan. Retrieved October 14, 2003, from http://www.disasterrecoveryworld.com/guidelines.htm

- Disasterplan.com. (n.d.). Disaster Recovery Planning - Have You Forgotten. Retrieved October 14, 2003 from http://www.disasterplan.com/yellowpages/Remember.html

- Federal Emergency Management Agency. (February 12, 2003). Emergency Management Guide For Business & Industry. Retrieved October 14, 2003 from http://www.fema.gov/library/bizindex.shtm

- National Institute of Standards and Technology. (June 2002). Contingency Planning Guide for Information Technology Systems. Retrieved October 14, 2003 from http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

- Massachusetts Institute of Technology. (1995). MIT Business Continuity Plan. Retrieved October 14, 2003 from http://web.mit.edu/security/www/pubplan.htm

- University of Missouri Records Management. (February 6, 1997). How to Prepare and Implement a Disaster Recovery Plan. Retrieved October 14, 2003 from http://www.system.missouri.edu/records/dpc5.html

- New York State Office of Mental Health. (January 13, 2003). Disaster Recovery Planning. Retrieved October 14, 2003 from http://www.omh.state.ny.us/omhweb/Institute/2002/postconference/session303A.htm

Last Updated: September 22nd, 2017

Upcoming Training

SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401^	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event