To Whom It May Concern,

We were requested to elaborate a Disaster Recovery Plan. We have analyzed the one provided by the SANS Institute and it fits our needs very adequately, so we have chosen to adopt their standards.

Please find their policies attached to this document.

We hope that resolves your questioning. Feel free to contact me for any clarification.

Kind regards,

Team 2.

[**SANS Institute**](http://www.sans.org/info/36909)

[Information Secu](http://www.sans.org/info/36909)rity Reading Room

**Disaster Recovery Plan**

**Strategies and Processes**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Bryan Martin

Copyright SANS Institute 2020. Author Retains Full Rights.

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Disaster Recovery Plan Strategies and Processes

Written by: Bryan C. Martin

February 2002

Version 1.3

# Introduction

This Disaster Recovery Plan is designed to ensure the continuation of vital business processes in the event that a disaster occurs. This plan will provide an effective solution that can be used to recover all vital business processes within the required time frame using vital records that are stored off -site. This Plan is just one of several plans that will provide procedures to handle emergency situations. These plans can be utilized individually but are designed to support one

another. The first plan is the Crisis Management Plan. This plan allows the ability to handle K y fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

high -level coordination activities surrounding any crisis situation. We will also discuss the development, maintenance and testing of the Disaster Recovery Plan. Lastly, we will discuss the culture and employee education on Disaster Recovery.

The term “disaster” is relative because disasters can occur in varying degrees. So, this Plan has considered this issue and incorporates management procedures as well as technical procedures to insure provable recovery capability.

The next key issue to be strongly considered within the strategy for disaster recovery is a recovery strategy for alternate processing (Hot-Site). This plan identifies discusses the Hot-Site and the alternatives if the primary location is not available to provide Disaster Recovery services for the various system environments.

The final issue to be addressed within the Disaster Recovery Strategy is to insure that every reasonable measure has been taken to identify and mitigate potential risks that exist within the processing environment.  ***The most successful Disaster Recovery Strategy is one that will never be implemented; therefore, risk avoidance is a critical element in the disaster recovery*** ***process.***

A Disaster Recovery Management System can be defined as the on-going process of planning, developing, testing and implementing Disaster Recovery management procedures and processes to ensure the efficient and effective resumption of vital business functions in the event of an unscheduled interruption. With the growing dependence on I/S and the Business Process to support business growth and changes associated with their complexities, compounded with the complexities of changing technology, the following elements are key to implementing a comprehensive Disaster Recovery Program:

**© SANS Institute 2002, Author retains full rights.**

· Critical Application Assessment

· Back-Up Procedures

· Recovery Procedures

· Implementation Procedures

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46· Test Procedures

· Plan Maintenance

# Crisis Management Plan

This Crisis Management Plan is designed to ensure the continuation of vital business processes in the event that an emergency or crisis situation should occur. H owever, Executives and Senior Management can use the procedures in this plan. Should an emergency situation occur at any of the business locations, the plan should provide an effective method that can be used by management personnel to control all activiti es associated with a crisis situation in a pro-active manner and to lessen the potential negative impact with the media, the public and with shareholders. This plan should be updated annually and should always be readily available to authorized personnel.

This plan is designed as a companion document to the Business Resumption Plan. The Business

Resumption Plan consists of two major parts, each a recovery plan. The first are the Disaster

Recovery Plans for technology in the event that a disaster should striKey fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46ke data processing center(s).

The second is the Business Recovery Plan that will address issues surrounding the business operation and business units should a disaster affect.

**© SANS Institute 2002, Author retains full rights.**

# Scope and Objectives of the Crisis Management Plan

The plan should provide in formation for the pro-active handling of any crisis situation and should include detailed procedures for the following:

* Executives
* Legal

* Investor Relations

* Corporate Communications
* Corporate Administration
* Marketing and Sales
* Human Resources
* Technology man agement

The plan should also document the responsibilities, procedures, and checklists that will be used to manage and control the situation following an emergency or crisis occurrence.

The Crisis Management Plan has been developed to accomplish the follo wing objectives:

* Prepare senior management personnel to respond effectively in a crisis situation;
* Manage the crisis in an organized and effective manner;
* Limit the magnitude or impact of any crisis situation to the various business units.

Crisis Manageme nt Plan activities are initiated by a situation or crisis alert procedure. After discovery of an incident, the Crisis Management Team will perform an assessment of the situation and determine if there is a need to declare an emergency or crisis and activat e the Crisis Management Plan. When the plan is activated, assigned management personnel will be alerted

and directed to activate their procedures.Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

# Disaster Definition

A “disaster” is any event that can cause a significant disruption in operational and/or computer processing capabilities for a period of time, which affects the operations of the business.

The purpose of defining a crisis or a discontinuity is to establish a documented description of what constitutes a crisis or a discontinuity. The inte nt is to minimize the decision-making process when an event occurs.

An outage (crisis/discontinuity) may exist when:

a. A service providing support to a critical business function fails.

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46b. It is determined the service cannot be restored before the point it beco mes vital to the business.

# Disaster Recovery Scenario

The disaster recovery scenario that will be specifically addressed, within the scope of this plan, is the loss of access to the computer center and the data processing capabilities of those systems and the network connectivity. Although loss of access to the facility may be more probable, this Disaster Recovery Plan will only address recovery of the critical systems and essential communications.

**© SANS Institute 2002, Author retains full rights.**

This scenario also assumes that all equipment in the computer room is not salvageable and that all critical telecommunications capability has been lost.

In the event of a declared Disaster, key personnel will take immediate action to alert the Disaster Recovery Center. Restoration of the Critical Coverage wi ll be provided after a Disaster is declared and after turnover of the disaster recovery backup site. It will include, without limitation, the following:

1. Delivery of the Authorized User Data and Software archived in off-site storage to the

Disaster Recovery Center

1. Connecting Network lines to the Disaster Recovery Center
2. Operating the Critical Applications on the Configuration at the Disaster Recovery Center 4. Provide Critical Coverage at the Disaster Recovery Center

5. Provide workspace and required equipment.

# Recovery Strategy

The recovery strategy that will be discussed as part of this Disaster Recovery Plan will be to relocate critical Information Systems processing to an alternate computer -processing center. The

processes will be recovered at the Disaster R ecovery Services provider name and location of the

HotKey fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46-Site. The Disaster Recovery Services provider name is responsible for ensuring that the

system configurations and the associated network requirements are accurate and technically feasible at all times. Therefore, yearly testing will be a part of the alternate processing strategy.

Also, the associated network connectivity will be recovered, within the disaster recovery scenario, using the alternate processing strategy.

# Recovery Phases

Recovery activit ies will be conducted in a phased approach. The emphasis will be to recover the critical applications effectively and efficiently. Critical applications will be recovered over a period of time after data center activation.

Phase I

Move operations to the Disaster Recovery Backup Site and the Emergency Operations Center. This activity will begin with activation of the Disaster Recovery Plan. There is a period of up to

24 hours allowed for organization and the turnover of the disaster recovery backup siteKey fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46 .

Phase II

To recover critical business functions, restoration of the critical applications and critical network connectivity. The goal here is to recover the systems and network so that our customers can continue business.

Phase III

Return data processing activities to the primary facilities or another computer facility.

The following conditions, if met, will constitute a successful recovery effort:

* Restore critical applications to the most current date available on backup tapes stored off -site. Updatin g the systems and databases will take place as the recovery effort progresses.
* It is understood that, due to the emergency or disaster, response times will probably be slower than normal production situations.

The Plan provides recovery procedures to be u sed at the present data center site after repairs have been made or at the Disaster Recovery Backup Site and the Emergency Operations Center. It also provides recovery procedures for the restoration of critical applications using either data recovered from the damaged data center or from the backup data stored off-site.

**© SANS Institute 2002, Author retains full rights.**

# Scope and Objectives of the Plan

The Disaster Recovery Plan provides a state of readiness allowing prompt personnel response after a disaster has occurred. This, in turn, provides for a more effective and efficient recovery effort. The Disaster Recovery Plan should be developed to accomplish the following objectives:

1. Limit the magnitude of any loss by minimizing the duration of a critical application service interruption.
2. Assess damage, repaKey fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46ir the damage, and activate the repaired computer center.
3. Recover data and information imperative to the operation of critical application’s.
4. Manage the recovery operation in an organized and effective manner.
5. Prepare technology personnel to respond effectively in disaster recovery situations.

Every business has the responsibility to respond to any short or long term disruption of services. By developing, documenting, implementing and testing this Disaster Recovery Plan, businesses will be able to restore the availability of critical applications in a timely and organized manner following a disaster occurrence. In order to accomplish these objectives, the technology area will depend on support from senior management, end users and staff departments.

Disas ter Recovery Plan activities are initiated by a situation or disaster alert procedure. After discovery of an incident, technology management will be informed of a potential disaster at the computer center. The Recovery Management Team will perform an asses sment of the situation and determine if there is a need to declare a disaster and activate the Disaster Recovery Plan. When the Plan is activated, assigned recovery personnel will be alerted and directed to activate their recovery procedures.Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

# Recovery Objectives

This section will define those applications and customers that are critical to the business and the

Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) for this Disaster Recovery Plan. The Recovery Time Objective is the length of time a business can be without data processing availability and the Recovery Point Objective (RPO) is how old the data will be once the systems are recovered.

The following applications and customers have been defined as critical and require restoration within the Recovery Time Objective (RTO) following a disaster declaration in order to support the restoration of the vital business functions. These applications and the supporting systems will be recovered within the Disaster Recovery Scenario using the alternate processing strategy. The list of Critical Applications and Critical Customers and the Recovery Time and Point Objectives should be reviewed and updated by management on an annual basis.

**© SANS Institute 2002, Author retains full rights.**

# Development of a Disaster Recovery Plan

1. Plan Scope and Objec tives
2. Business Recovery Organization (BRO) and Responsibilities (Recovery Team Concept)
3. Major Plan Components - format and structure
4. Scenario to Execute Plan
5. Escalation, Notification and Plan Activation
6. Vital Records and Off -Site Storage Program
7. Personnel Control Program
8. Data Loss Limitations
9. Plan Administration (general)

# Maintenance of the Plan

The purpose of this section is to define the activity necessary to maintain the Disaster Recovery

(DR) Plan for the mainframe anKey fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46d mid-range environments. DR Plan maintenance is of utmost

importance to ensure currency of what is to be recovered and procedures governing the recovery. This means keeping the test plan and implementation plan current and in sync with business changes. All changes to the business and in the mainframe and mid-range environments must be considered for inclusion in and for updating of the Disaster Recovery Plan.

The Disaster Recovery Plan may require updates if problems or changes include some or any of the following:

* Mainframe and Mid-Range Disaster Recovery Test results
* New critical applications or critical customers
* Increased application complexity
* New equipment acquisitions - Changes to:
* Hardware
* Software
* Network

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46- Applications

* Data

A formal review of a Disaster Recovery Plan should be conducted yearly, and a quarterly Disaster Recovery Readiness Assessment Audit should be conducted as well. The purpose of the reviews and the audits is to identify any changes to ensure tha t these and any other updates identified since the previous review have been captured.

**© SANS Institute 2002, Author retains full rights.**

Items to be reviewed for Plan update should include:

* Personnel changes
* Mission changes
* Priority changes
* New Business Organizations
* Mainframe and Mid-range Disaster Recovery Test procedures and results
* Backup procedures
* Recovery procedures
* Relocation / Migration Plan
* Software (operating system, utilities, application programs)
* Hardware (mainframe, mid-range and peripherals)
* Communications Network Facilities

Particular attention should be paid to the review of the recovery equipment configurations to ensure that the business has the required equipment to restore the business functionality as quickly and smoothly as possible.

These reviews will require the time and attention of all Plan holders and team members, especially those that have hardware and network responsibilities.

The proper maintenance of the Plan will be the responsibility of ALL holders of the Plan. It will be their responsi bility to incorporate all approved revisions into their assigned copy to ensure

that the Plan manual is maintained as a viable and readied Action Plan. All removed pages are to Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

be properly disposed; they should be placed in the classified materials bins th roughout the office or shredded. It is the responsibility of all Plan holders to protect Confidential material and dispose of it in a proper manner.

# Disaster Recovery Testing Overview

The purpose of this Test Plan Document is to specifically identify and document the task plan and procedures to be implemented in a testing environment. This Test Plan includes test parameters, objectives, measurement criteria, test methodology, task plan charts and time lines to validate the effectiveness of the current Di saster Recovery Plan. The Disaster Recovery Plan will be tested to ensure that the business has the ability to continue the critical business processes in the event of a disaster. It is very important that the Recovery procedures are executable and accurat e. Another benefit of testing the plan is to train the personnel who will be responsible for executing the Disaster Recovery Plan. The important issue is not that the test succeeded without problems, but, that the test results and problems encountered are reviewed and used to update or

**© SANS Institute 2002, Author retains full rights.**

revise the current Disaster Recovery Plan procedures. Testing can be accomplished by executing Key finge print = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

the disaster implementation plan or it may be desirable to execute a subset of the plan. When performing a Disaster Recovery Test , it is very important to use only that information which is recalled from the off -site storage facility. This is to ensure the following:

1. Simulate the conditions of an ACTUAL Disaster Recovery situation.
2. Completeness of the disaster recovery information stored at the Records Retention

Site.

1. Ensure the ability to recover the intended functions.

This test plan includes the following areas:

* 1. Schedule
     1. Planning Sessions
     2. Pre-Test Technical Review
     3. Debriefing
  2. Introduction
     1. Preface
     2. Scope
     3. Recovery Site
     4. Primary Test Objectives
     5. Secondary Test Objectives
     6. Exclusion (if applicable)
     7. Test Assumptions, Dependencies and Success Criteria
  3. Test Teams
     1. ChoicePoint Participants
     2. IBM Participants (as applicable)  4. Pre-Test Planning
     3. Activities
     4. Issues

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46 c. Concerns

5. Test Timeline

* + 1. Planned start and stop time of test and tasks.
    2. Actual start and stop time of test and tasks (to be completed during the test)

6. Critical Test Checkpoints

* + 1. Activity
    2. Recommendation
    3. Responsible party

7. Test Problem Log

* + 1. Document any problems encountered prior to the test.
    2. Record any deviations from Test Plan.

# Post Test Review

The purpose of this Post Test Review document is to identify any problem areas and any recommendations for improvement to the plan. The Post Test Review document includes the following areas:Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

**© SANS Institute 2002, Author retains full rights.**

1. Highlights
   1. Overall Test Results
   2. Test Dates
   3. Disaster Recovery Back-up Site
   4. Local Access Suite
   5. Test Participants
2. Test Objectives
   1. Primary Test Objectives
   2. Secondary Test Objectives
   3. Exclusions (if applicable)
3. Timeline
   1. Planned task, start and end times and duration
   2. Actual task, start and end times 4. Problems Encountered During the Test

a. Problem Log

* + 1. Actual Problem
    2. Assigned to
    3. Target Date for Resolution
    4. Status
    5. Resolution
    6. DR Process or Technical

b. Problem Summary

1. Follow Up to Pre-Test Problems
2. Follow Up to Suggestions for Improvement/Recommendations from Last Year's

Test

1. Detailed Summary and Observations
2. Recommendations for Next Year's Test

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

# Establishing the Continuity Culture

Documenting the Disaster Recovery Plan is one element of developing a strategy. The plan’s success, however, depends upon:

* Implementation of the recommendations made, across the entire business.
* A program of training of those directly involved in the execution of the

plan

* An education and awareness program to ensure enterprise-wide understanding and adoption of the plan, covering internal and external stakeholders, i.e. employees, customers, suppliers and shareholders

It is essential to commit to implementing all recommendation s and strategies identified in the

Disaster Recovery Plan, otherwise investment made in its preparation will be redundant. Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

Similarly training and awareness must be embarked upon to ensure that the entire organization is confident and competent concerning t he plan. All parties must appreciate the importance of Disaster Recovery Plan to the operation’s survival and their role in this process.

This awareness should extend to those external stakeholders and third parties upon whom the organization depends/has influence in both normal and crisis operations.

Implementation of the plan in this manner and all those associated with the organization can have confidence in its ability to manage in a crisis, and the continuity culture will have started.

**Actions:**

* Select the Emergency Management/ BCM/ Crisis and Recovery

Teams.

* Implement relevant training programs for each team dependent upon task, including crisis communications/ media training as appropriate.

This process is ongoing, as team members will change.

* Establish and equip emergency and crisis centers.

* Establish internal and external contractual arrangements/ service level

agreements.

* Implement back-up and off-site storage arrangements.
* Distribute plan documentation as appropriate.
* Conduct internal and external awareness programs. These programs can be built into employee and supplier induction processes and customer marketing programs.

**© SANS Institute 2002, Author retains full rights.**

**Disaster Recovery Education for Employees:**

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46 **Prepare Your Employees for Data Backup:**

You'll need to educate your employees about where to store their files (in a specific directory on their PC that is backed up or on the central server) so that all files are included in the backup.

You'll also want to avoid data loss and downtime by installing anti -virus software and teaching your employees how viruses are spread and

**Prepare your Employees for Disaster Recovery:**

Involving employees in the disaster recovery effort will also help ensure that recovery procedures are well planned and executed based on your business' need to provi de as seamless a recovery as possible. Find out typical processes and turnaround times that your customers have come to expect and plan how you will prioritize recovery efforts. Make sure all employees know whom to contact in an emergency, and outline what they can do to remain productive during the recovery period. If you're using a service, identify who in the company will contact the service to initiate recovery efforts. Make sure you have the contact information off -site in case of a fire, flood, or oth er act of nature.

**© SANS Institute 2002, Author retains full rights.**

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46 **Disaster Recovery Statistics:**

* Only 15% of midrange data centers would be able to recover more than 30% of their applications in any time frame.
* Just 3.8% could recover their applications within the same day.
* Only 2.5% could recover within four hours.

# The eight R’s of a successful recovery plan

* Reason for planning
* Recognition
* Reaction
* Recovery
* Restoration
* Return To Normal

* Rest and Relax

* Re-evaluate and Re-document

# Conclusion

Every day, businesses are confronted with disasters of varying degrees. Those that have

adequately developed, maintained, and exercised their contingency plans will survive. Yet many

corporate executives continue to take the uninhibited operations of their companies for granted.

They remain complacent, assuming that the power will always be available, the telephone system

will not fail, there will be no fire or earthquake--everything will always be normal. Very few

executives plan for their own, much less their organization’s mortality; however, if a business is

to survive, organizational “strategic” and “tactical” battle planning is essential. The final

corporate contingency plan is the lifeblood of corporate survival. However, it is only as good as

the foundation upon which it was built. The foundation is, of course, the concept. This document

is the means by which a particular mission, program, or policy directive is translated into a

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

fundamental organizational and operational methodology. Once the concept is developed

through a logical building block approach, and is sanctioned by both management and the operating elements, construction of the contingency plan may commence. A fundamental premise of successful contingency planning is that plans are developed by those who must actually carry them out in the event of a n actual disaster. The role of the Corporate Contingency Planner is to strategically, and relentlessly, manage the process. And, in doing so, he or she must rely on both internal and external assistance. In addition to in-house assistance, there are a mult itude of disaster assistance organizations and services available to assist the contingency planner. Preparing a corporate contingency plan is a non -trivial undertaking. However, corporate leaders must recognize the vulnerabilities they invite by not adequ ately planning for survival. Disaster planning is truly a vital part of the overall business plan.

**References:**

1. Wold, Geoffrey H. “Disaster Recovery Planning Process”

http://www.drj.com/new2dr/Key fingerprint = AF19 FA27 2F94 998w2\_004.htmD FDB5 DE3D F8B5 06E4 A169 4E46

1. The Business Continuity Institute http://www.thebci.org/frametrial.html

1. Boroski, Doran. “ Protect processes as well as investments in disaster recovery plans” http://www.computerworld.com/storyba/0,4125,NAV47\_STO68345,00.html

1. DRI International ”Business Continuity Management Survey Examines How The Events of 9/11 Shape the Bus iness Continuity Industry” http://www.dr.org/fallnews.pdf

**© SANS Institute 2002, Author retains full rights.**

1. Wrobel, Len “Components of a Successful LAN Disaster Recovery Plan” http://www.disaster -resource.com/content\_page/nuggets.shtml

1. Radeke, Michelle “Prepare for Effective Data Backup and Recovery” http://www.workz.com/content/543.asp

1. Hussong, Jr. W illiam A. “So You’re The Company’s New Contingency Planner” http://www.drj.com/new2dr/w3\_001.htm

1. Disaster Recovery Planning: Strategies for Protecting Critical Information Assets By: Jon William Toigo

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

**© SANS Institute 2002, Author retains full rights.**

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

Last Updated: February 15th, 2020

[**Upcoming SANS Training**](http://www.sans.org/courses?utm_source=Print&utm_medium=Reading+Room+Paper&utm_content=Disaster_Recovery_Plan_Strategies_and_Processes+Cover&utm_campaign=SANS+Courses)

[**Click here to view a list of all SANS Courses**](http://www.sans.org/courses?utm_source=Print&utm_medium=Reading+Room+Paper&utm_content=Disaster_Recovery_Plan_Strategies_and_Processes+Cover&utm_campaign=SANS+Courses)

|  |  |  |  |
| --- | --- | --- | --- |
| [**SANS Scottsdale 2020**](http://www.sans.org/link.php?id=60265&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Scottsdale_2020) | **Scottsdale, AZUS** | **Feb 17, 2020 - Feb 22, 2020** | [**Live Event**](http://www.sans.org/link.php?id=60265&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Scottsdale_2020) |
| [**SANS San Diego 2020**](http://www.sans.org/link.php?id=60270&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_San_Diego_2020) | **San Diego, CAUS** | **Feb 17, 2020 - Feb 22, 2020** | [**Live Event**](http://www.sans.org/link.php?id=60270&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_San_Diego_2020) |
| [**Open-Source Intelligence Summit & Training 2020**](http://www.sans.org/link.php?id=59880&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=Open-Source_Intelligence_Summit_Training_2020) | **Alexandria, VAUS** | **Feb 18, 2020 - Feb 24, 2020** | [**Live Event**](http://www.sans.org/link.php?id=59880&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=Open-Source_Intelligence_Summit_Training_2020) |
| [**SANS Training at RSA Conference 2020**](http://www.sans.org/link.php?id=62750&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Training_at_RSA_Conference_2020) | **San Francisco, CAUS** | **Feb 23, 2020 - Feb 24, 2020** | [**Live Event**](http://www.sans.org/link.php?id=62750&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Training_at_RSA_Conference_2020) |
| [**SANS Secure India 2020**](http://www.sans.org/link.php?id=59845&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Secure_India_2020) | **Bangalore, IN** | **Feb 24, 2020 - Feb 29, 2020** | [**Live Event**](http://www.sans.org/link.php?id=59845&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Secure_India_2020) |
| [**SANS Zurich February 2020**](http://www.sans.org/link.php?id=58170&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Zurich_February_2020) | **Zurich, CH** | **Feb 24, 2020 - Feb 29, 2020** | [**Live Event**](http://www.sans.org/link.php?id=58170&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Zurich_February_2020) |
| [**SANS Manchester February 2020**](http://www.sans.org/link.php?id=58460&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Manchester_February_2020) | **Manchester, GB** | **Feb 24, 2020 - Feb 29, 2020** | [**Live Event**](http://www.sans.org/link.php?id=58460&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Manchester_February_2020) |
| [**SANS Jacksonville 2020**](http://www.sans.org/link.php?id=60275&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Jacksonville_2020) | **Jacksonville, FLUS** | **Feb 24, 2020 - Feb 29, 2020** | [**Live Event**](http://www.sans.org/link.php?id=60275&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Jacksonville_2020) |
| [**ICS Security Summit & Training 2020**](http://www.sans.org/link.php?id=59885&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=ICS_Security_Summit_Training_2020) | **Orlando, FLUS** | **Mar 02, 2020 - Mar 09, 2020** | [**Live Event**](http://www.sans.org/link.php?id=59885&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=ICS_Security_Summit_Training_2020) |
| [**SANS Secure Japan 2020**](http://www.sans.org/link.php?id=59745&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Secure_Japan_2020) | **Tokyo, JP** | **Mar 02, 2020 - Mar 14, 2020** | [**Live Event**](http://www.sans.org/link.php?id=59745&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Secure_Japan_2020) |
| [**Blue Team Summit & Training 2020**](http://www.sans.org/link.php?id=60595&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=Blue_Team_Summit_Training_2020) | **Louisville, KYUS** | **Mar 02, 2020 - Mar 09, 2020** | [**Live Event**](http://www.sans.org/link.php?id=60595&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=Blue_Team_Summit_Training_2020) |
| [**SANS Northern VA - Reston Spring 2020**](http://www.sans.org/link.php?id=60360&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Northern_VA_-_Reston_Spring_2020) | **Reston, VAUS** | **Mar 02, 2020 - Mar 07, 2020** | [**Live Event**](http://www.sans.org/link.php?id=60360&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Northern_VA_-_Reston_Spring_2020) |
| [**SANS Munich March 2020**](http://www.sans.org/link.php?id=58920&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Munich_March_2020) | **Munich, DE** | **Mar 02, 2020 - Mar 07, 2020** | [**Live Event**](http://www.sans.org/link.php?id=58920&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Munich_March_2020) |
| [**SANS Jeddah March 2020**](http://www.sans.org/link.php?id=58470&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Jeddah_March_2020) | **Jeddah, SA** | **Mar 07, 2020 - Mar 12, 2020** | [**Live Event**](http://www.sans.org/link.php?id=58470&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Jeddah_March_2020) |
| [**SANS St. Louis 2020**](http://www.sans.org/link.php?id=60450&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_St_Louis_2020) | **St. Louis, MOUS** | **Mar 08, 2020 - Mar 13, 2020** | [**Live Event**](http://www.sans.org/link.php?id=60450&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_St_Louis_2020) |
| [**SANS Paris March 2020**](http://www.sans.org/link.php?id=58665&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Paris_March_2020) | **Paris, FR** | **Mar 09, 2020 - Mar 14, 2020** | [**Live Event**](http://www.sans.org/link.php?id=58665&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Paris_March_2020) |
| [**SANS Dallas 2020**](http://www.sans.org/link.php?id=60455&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Dallas_2020) | **Dallas, TXUS** | **Mar 09, 2020 - Mar 14, 2020** | [**Live Event**](http://www.sans.org/link.php?id=60455&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Dallas_2020) |
| [**SANS Prague March 2020**](http://www.sans.org/link.php?id=58180&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Prague_March_2020) | **Prague, CZ** | **Mar 09, 2020 - Mar 14, 2020** | [**Live Event**](http://www.sans.org/link.php?id=58180&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Prague_March_2020) |
| [**Wild West Hackin Fest 2020**](http://www.sans.org/link.php?id=63315&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=Wild_West_Hackin_Fest_2020) | **San Diego, CAUS** | **Mar 10, 2020 - Mar 11, 2020** | [**Live Event**](http://www.sans.org/link.php?id=63315&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=Wild_West_Hackin_Fest_2020) |
| [**SANS Doha March 2020**](http://www.sans.org/link.php?id=58465&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Doha_March_2020) | **Doha, QA** | **Mar 14, 2020 - Mar 19, 2020** | [**Live Event**](http://www.sans.org/link.php?id=58465&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Doha_March_2020) |
| [**SANS Norfolk 2020**](http://www.sans.org/link.php?id=60460&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Norfolk_2020) | **Norfolk, VAUS** | **Mar 16, 2020 - Mar 21, 2020** | [**Live Event**](http://www.sans.org/link.php?id=60460&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Norfolk_2020) |
| [**SANS SEC504 Nantes March 2020 (in French)**](http://www.sans.org/link.php?id=60530&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_SEC504_Nantes_March_2020_in_French) | **Nantes, FR** | **Mar 16, 2020 - Mar 21, 2020** | [**Live Event**](http://www.sans.org/link.php?id=60530&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_SEC504_Nantes_March_2020_in_French) |
| [**SANS Secure Singapore 2020**](http://www.sans.org/link.php?id=55490&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Secure_Singapore_2020) | **Singapore, SG** | **Mar 16, 2020 - Mar 28, 2020** | [**Live Event**](http://www.sans.org/link.php?id=55490&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Secure_Singapore_2020) |
| [**SANS San Francisco Spring 2020**](http://www.sans.org/link.php?id=60590&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_San_Francisco_Spring_2020) | **San Francisco, CAUS** | **Mar 16, 2020 - Mar 27, 2020** | [**Live Event**](http://www.sans.org/link.php?id=60590&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_San_Francisco_Spring_2020) |
| [**SANS London March 2020**](http://www.sans.org/link.php?id=59001&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_London_March_2020) | **London, GB** | **Mar 16, 2020 - Mar 21, 2020** | [**Live Event**](http://www.sans.org/link.php?id=59001&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_London_March_2020) |
| [**SANS Kuwait March 2020**](http://www.sans.org/link.php?id=62945&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Kuwait_March_2020) | **Salmiya, KW** | **Mar 21, 2020 - Mar 26, 2020** | [**Live Event**](http://www.sans.org/link.php?id=62945&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Kuwait_March_2020) |
| [**SEC588 Beta One 2020**](http://www.sans.org/link.php?id=63985&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SEC588_Beta_One_2020) | **Arlington, VAUS** | **Mar 23, 2020 - Mar 28, 2020** | [**Live Event**](http://www.sans.org/link.php?id=63985&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SEC588_Beta_One_2020) |
| [**SANS Seattle Spring 2020**](http://www.sans.org/link.php?id=60575&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Seattle_Spring_2020) | **Seattle, WAUS** | **Mar 23, 2020 - Mar 28, 2020** | [**Live Event**](http://www.sans.org/link.php?id=60575&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Seattle_Spring_2020) |
| [**SANS Oslo March 2020**](http://www.sans.org/link.php?id=58925&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Oslo_March_2020) | **Oslo, NO** | **Mar 23, 2020 - Mar 28, 2020** | [**Live Event**](http://www.sans.org/link.php?id=58925&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Oslo_March_2020) |
| [**SANS Madrid March 2020**](http://www.sans.org/link.php?id=58195&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Madrid_March_2020) | **Madrid, ES** | **Mar 23, 2020 - Mar 28, 2020** | [**Live Event**](http://www.sans.org/link.php?id=58195&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Madrid_March_2020) |
| [**SANS SEC560 Lyon March 2020 (In French)**](http://www.sans.org/link.php?id=60715&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_SEC560_Lyon_March_2020_In_French) | **Lyon, FR** | **Mar 23, 2020 - Mar 28, 2020** | [**Live Event**](http://www.sans.org/link.php?id=60715&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_SEC560_Lyon_March_2020_In_French) |
| [**SANS Secure Canberra 2020**](http://www.sans.org/link.php?id=55495&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Secure_Canberra_2020) | **Canberra, AU** | **Mar 23, 2020 - Mar 28, 2020** | [**Live Event**](http://www.sans.org/link.php?id=55495&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Secure_Canberra_2020) |
| [**SANS Brussels February 2020**](http://www.sans.org/link.php?id=58155&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Brussels_February_2020) | **OnlineBE** | **Feb 17, 2020 - Feb 22, 2020** | [**Live Event**](http://www.sans.org/link.php?id=58155&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_Brussels_February_2020) |
| [**SANS OnDemand**](http://www.sans.org/link.php?id=1032&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_OnDemand) | **Books & MP3s OnlyUS** | **Anytime** | [**Self Paced**](http://www.sans.org/link.php?id=1032&rrpt=Disaster_Recovery_Plan_Strategies_and_Processes&rret=SANS_OnDemand) |