NOT FOR PUBLIC RELEASE

Disaster Recovery Business Continuity Template

Version 8.0

Table of Contents[1]

[1] NOTE – Due to incompatibilities between WORD 2003 and WORD 2007 you may need to regenerate the Table of Contents. The Table of Contents was generated using WORD 2007 and if you use this document in any version other than WORD 2007 you will have to update the Table of Contents and all update fields which link to unique pages in this template.

1.0 Plan Introduction

ENTERPRISE recognizing their operational dependency on computer systems, including the Local Area Network (LAN), Database Servers, Internet, Intranet and e-Mail, and the potential loss of revenue and operational control that may occur in the event of a disaster; authorized the preparation, implementation and maintenance of a comprehensive disaster recovery plan.

The intent of a Disaster Recovery Plan is to provide a written and tested plan directing the computer system recovery process in the event of an interruption in continuous service resulting from an unplanned and unexpected disaster.

The Disaster Recovery Plan preparation process includes several major steps as follows:

- Identify Systems and Applications currently in use
- Analyze Business Impact of computer impact and determination of critical recovery time frames
- Determine Recovery Strategy
- Document Recovery Team Organization
- Document Recovery Team Responsibilities
- Develop and Document Emergency Procedures
- Document Training & Maintenance Procedures

These steps were conducted and this document represents the completed effort in the preparation of the ENTERPRISE Disaster Recovery Plan.

1.1 Mission and Objectives

The mission of the Disaster Recovery Plan is to establish defined responsibilities, actions, and procedures to recover the ENTERPRISE computer, communication, and network environment in the event of an unexpected and unscheduled interruption. The plan is structured to attain the following objectives:

- Recover the physical network within the Critical Time Frames[2] established and accepted by the user community
- Recover the applications within the Critical Time Frames established and accepted by the user community
- Minimize the impact on the business with respect to dollar losses and operational interference

Compliance

Various compliance frameworks can be used to assess BCP measures—ISO, COBIT, COSO, etc.—but key aspects are similar:

- COSO requires data center operation controls and transaction management controls in order to ensure data integrity and availability.
- ISO 1799 has a section entitled Business Continuity Management that requires testing, maintaining, and reassessing a business continuity plan.
- ISACA's COBIT requires uninterruptible power supplies under its Manage Facilities section.
- NIST requires contingency and continuity plans and management.

As a general rule, in order to test BCP/DR compliance within an organization, a team of qualified, knowledgeable internal auditors should be created, reporting to a different member of the board than the BCP team reports to. This team of internal auditors should test to ensure that the BCP plan and process meet the compliance requirements discussed in the following sections.

Implication of Legislated and Industry Standards Requirements

There[3] are a number of legally mandated and standards mandated issues that need to be covered in the Disaster Recovery / Business Continuity Planning Process.

In addition to the Security & Exchange Commission (SEC) requirements of Sarbanes-Oxley, there are PCI DSS requirements issued by credit card companies, security requirements of HIPAA, and individual state requirements (California and New York) that needed to be considered in the plan.

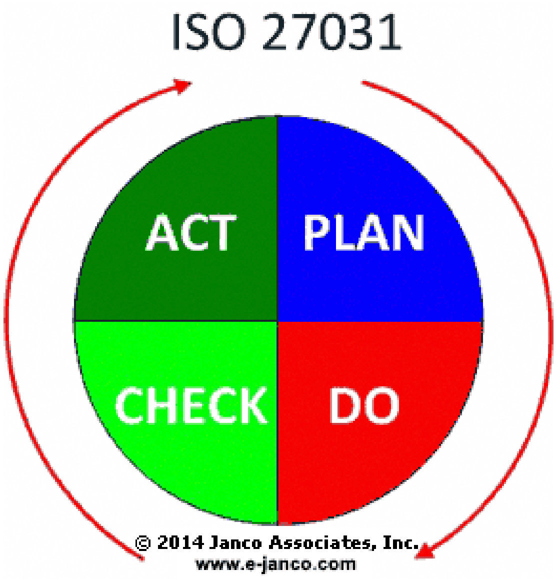
[2] Critical time frames include both the point in time that the recovery will be set to and the point in time that the recovery will be completed and the enterprise can be back in operation.

[3] This section is for informational purposes and can be excluded from the plan.

ISO 27031 Overview

The ISO Standard defines the Information and Communication Technology (ITC) Requirements for Business Continuity (IRBC) program that supports the mandate for an infrastructure that supports business operations when an event or incident with its related disruptions affect the continuity of critical business functions. This includes security of crucial data as well as enterprise operations.

The ISO standard centers around four areas; Plan, Do, Check, and Act.

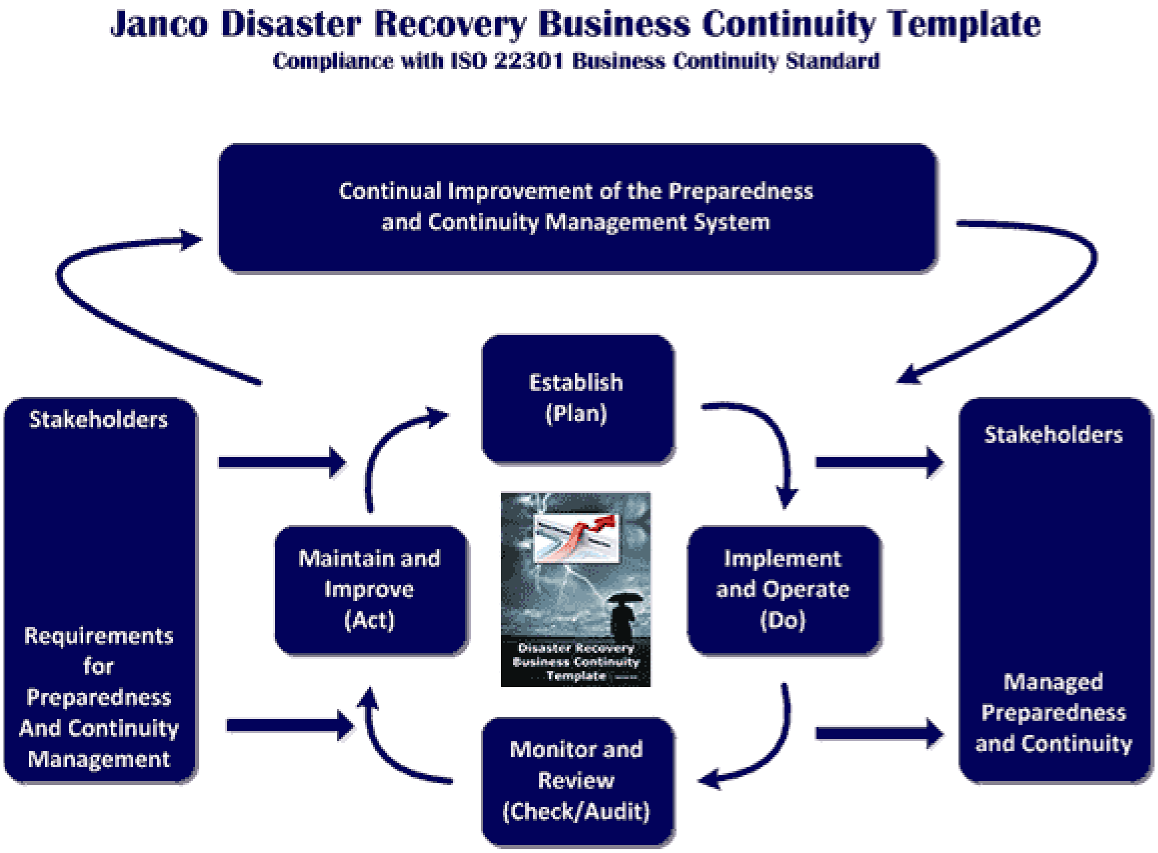


- **Plan** - Establish a Disaster Recovery Business Continuity policy. with objectives, metrics, processes relevant to managing risk and improving Information and Communication Technology's ability and readiness to operate at the level defined within the parameters of the enterprises overall disaster recovery and business continuity objectives.
- **Do** - Implement and operate the Disaster Recovery and Business Continuity policies, procedures, controls an processes.
- **Check** - Assess and monitor the performance metrics as defined within the Disaster Recovery and Business Continuity policy and metrics and communicate the results to the management of the enterprise.
- **Act** - Modify the Disaster Recovery and Business Continuity policies, procedures and metrics based on the "Check" in order to improve the Disaster Recovery and Business Continuity Policy.

- Suppliers
  - Vendor and Supplier Disaster Recovery Questionnaire (Appendix)
  - Disaster Recovery Sample Contract (Appendix)

ISO 22301

ISO 22301 is the latest ISO Business Continuity standard. It is called "Societal security – Business continuity management systems – Requirements". Although societal security may sound a little strange in relation to business continuity, here is how ISO defines it: … standardization in the area of societal security, aimed at increasing crisis management and business continuity capabilities, i.e. through improved technical, human, organizational, and functional interoperability as well as shared situational awareness, amongst all interested parties.



Janco Disaster Recovery Business Continuity Template

Compliance with ISO 22301 Business Continuity Standard

Continual Improvement of the Preparedness and Continuity Management System
Stakeholders
Requirements for Preparedness And Continuity Management
Establish (Plan)
Implement and Operate (Do)
Monitor and Review (Check/Audit)
Maintain and Improve (Act)
Disaster Recovery Business Continuity Template
Stakeholders
Managed Preparedness and Continuity

2.0 Business Impact Analysis

A Business Impact Analysis was conducted to ascertain the impact of a disaster on the operations of each operating unit within ENTERPRISE. The Business Impact Analysis drives the Disaster Recovery Plan by identifying and substantiating those applications and systems with the greatest impact on the business in the event of a disaster.

In turn, this provides for the determination of the most cost effective recovery time-period for each system and application. Recovery times are established and accepted by the user community.

2.1 Scope

The scope of the Business Impact Analysis is the ENTERPRISE operating departments supported by data center facilities located at ____________ ______________________________. This network encompasses the following information technology services:

- General business applications, such as word-processing, spreadsheet and database applications
- e-Mail
- File servers supporting all business operations
- Gateway to the supplier applications and other sites
- WEB / e-commerce processing
- Wireless Networks
- Mobile applications and BYOD devices
- Non-ENTERPRISE infrastructure including power grids, telephone switching centers, microwave towers, and cell and wireless transmission sites within a ten (10) mile radius of the facility

To determine the maximum time frame allowable, the following ENTERPRISE operating departments were interviewed (See Appendix - People Interviewed):

- Information Technology
- Sales
- Marketing
- Credit
- Finance
- Human Resources
- Manufacturing
- Distribution
- Customer Service
- Accounting
- Investor Relations

3.0 Backup Strategy

Considering the wide-ranging geographic impact certain disastrous events can have (large scale power outages, floods, blizzards, hurricanes, tornadoes, etc.) it has become a standard practice to keep data backups in significantly disparate locations. However, when a business interruption does occur, it is imperative for the enterprise to recover key information as quickly as possible.

With ENTERPRISE data stored at remote ISP[10] , personal desktops, laptops, and PDA[11] in addition to file servers and legacy mainframe processing centers a strategy for backing widely scattered information. Based on the size of the operation and the need for recovery of the data the following backup strategy should be implemented. Strategies for each are discussed in the sections that follow for:

- Communication Strategy and Policy
- ENTERPRISE Data Center Systems
- Departmental File Servers
- Wireless Network File Servers
- Data at Outsourced Sites (including ISP's)
- Desktop Workstations (In Office)
- Desktop Workstations (Off site including at home users)
- Laptops
- PDA's
- BYOD

3.01 Site Strategy

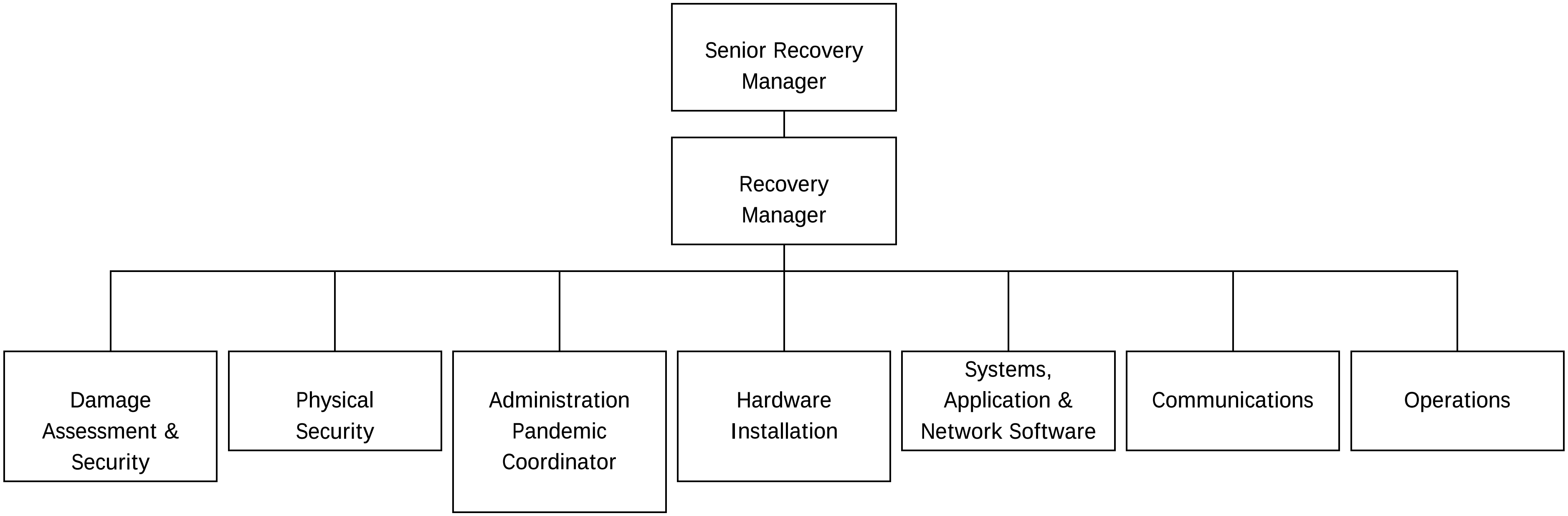
Most organizations have more than one recovery site strategy in place, since different business processes have different cost factors and service-level requirements. For example, for data center operations with large capital investments in hardware required for a secondary site, a shared-cost commercial hot-site service provider may be the most effective option. In contrast, provisioning of client-side alternate workspace may be more economically and effectively provisioned internally. Recovery time objectives ("How quickly do I need to be back online?") and data currency objectives ("How much data can the enterprise afford to lose?") will often place restrictions on recovery site options.

[10] Internet Service Providers and other "outsourced" service providers.

[11] Personal Digital Assistants

Recovery Strategy	Recovery Time	Advantages	Disadvantages	Comments
Commercial Hot site	24 to 48 Hours	- Best recovery time - Easiest to implement as equipment, application software, data, and OS are in place - Easy to test at any point in time - Best solution that is available to support on-going operations	- Most expensive options duplicate equipment and software plus on going version control issues - Ongoing communication costs to duplicate data very high - Term of the agreement can limit duration of use - If you are not the "most important customer" you could be bumped	Often the most cost effective strategy for data center recovery strategies.. Clear contract terms need to be defined which meets the enterprise service objectives. Consideration should be made for disasters which impact entire regions such as hurricanes and earthquakes.
Internal Hot site	1 to 12 hours	- Best recovery time - Easiest to implement as equipment, application software, data, and OS are in place - Easy to test at any point in time - Best solution that is available to support on-going operations	- Most expensive options duplicate equipment and software plus on going version control issues - Ongoing communication costs to duplicate data very high	If costs can be shared among multiple facilities within the enterprise, internal provisioning can be cost competitive with commercial alternatives. If no appropriate secondary space is available "co-location" facilities providers offer managed raised-floor space at very attractive rates as an alternative to building out secondary sites.
Warm Site	24 to 48 Hours	- Moderately priced - Basic infrastructure is in place to support recovery operations - Ability to pre-stage delivery and implementing of necessary hardware, application software, OS software, data, and communications	- Not easy to test - Recovery time is longer than with hot site and is controlled by the time to locate and restore applications - Facility equipment may not be exactly what is required – Once the recovery begins delays may occur because of equipment, software, or staffing shortfalls	If costs can be shared among multiple facilities within the enterprise, internal provisioning can be cost competitive with commercial alternatives. If no appropriate secondary space is available "co-location" facilities providers offer managed raised-floor space at very attractive rates as an alternative to building out secondary sites.
Mobile Site	24 to 48 Hours	- Moderately priced - Typically can be in place with 36 to 72 hours - Can be placed in the "parking lot" adjacent to you impacted facility	- Recovery time typically is at least 2 to 5 days longer than a hot site. - Access to your impacted facility may be hindered because of the event - Trailer may not be configured exactly as you need it	This approach avoids employee travel issues but has limitations on equipment availability and outbound bandwidth if very small aperture satellite terminal (VSAT) links must be used for communications. If the disaster profile includes events such as hurricanes, floods or toxic spills, these solutions may not be appropriate.
Cold Site	72 plus Hours	- Lowest cost solution - Basic infrastructure power, air, and communication are in place - Can rent the facility for a longer term at lower cost	- Longest recovery time - All equipment must be order, delivered, installed and made operational - Worst solution for supporting on-going operations	"Environmentally appropriate" space can be either provisioned internally or contracted from a commercial facilities service provider. Cold-site strategies are usually based on "quick-ship" delivery agreements to allow server, storage, and communications hardware and network service providers to quickly build out the data center and/or client workspace infrastructure.
Reciprocal Agreement	12 to 48 Hours	- Least costly solution - Better than no strategy	- Seldom works - Typically in the same geographic area and a wide range disaster like an earthquake renders it of no use - No easy way to test	This is typically a formal agreement between two trusted, non-competing partners in different industries in which each provides secure sites for the other. This option is the least favorable and has the greatest risk associated with it.
Cloud	0 to 24 Hours	- Data and applications available immediately - Location independent - Easy to test	- Security - May not allow enough time for a daily cycle processing window	Data should be in place so activation would only be limited by connectivity and network addressing (DNS propagation).

5.1 Recovery Team Organization Chart


Senior Recovery Manager
Recovery Manager
Damage Assessment & Security
Physical Security
Administration Pandemic Coordinator
Hardware Installation
Systems, Application & Network Software
Communications
Operations

8.03 Disaster Recovery – Business Continuity Team Call List

This call list should be updated at least monthly and whenever there is any organizational changes or new personnel assume any of these roles

Role	Individual	Office Phone	Email	Mobile	Alternate Email	Credit Card Issued
Recovery Manager Senior						□ Yes □No
Recovery Manager						□ Yes □No
Damage Assessment						□ Yes □No
Physical Security						□ Yes □No
Administration						□ Yes □No
Hardware						□ Yes □No
Network						□ Yes □No
Application Software						□ Yes □No
Communication						□ Yes □No
Operations						□ Yes □No
Customer Relations						□ Yes □No
Supplier Relations						□ Yes □No
Vendor Relations						□ Yes □No
Media Communications						□ Yes □No

Completed by:

Department:

Date:

Enterprise logo here

Application / File Servers

Provide the following information for each application and file server:

- Host name
- IP address and mask for the server
- Administrative contact for the server and security contact (i.e. primary user or department head name and phone number)
- User Types
- Operating system including version number
- Application Software including version number
- Review status (Yes/No, Date. Reviewer)
- Connectivity (Internet, Intranet, modem In, modem out, other
- Physical location (Address / phone number for contact

Host Name: ___________________________		**Reviewer Name:** _________________________________		**Date:** __________________
IP Address / Mask	**User Types**	**Administrative Contact**	**Connectivity**	**Physical Location**
___.___.___.___ ___.___.___.___ **(mask)**	☐ Public ☐ Customers ☐ Employees ☐ Groups Employees ☐ Specific Employees ☐ ______________	Name: ______________________ Email: ______________________ Phone: _____________________	☐ Internet ☐ Intranet ☐ Modem In Bound ☐ Modem Out Bound ☐ Other: ____________	Address: _________________ Contact::_________________ Phone: __________________
IP Address Range	**Operating System**	**OS Version / Reviewed**	**Application**	**App Version / Reviewed**
___.___.___.___ to ___.___.___.___	☐ Windows WS ☐ Windows Server ☐ Unix ☐ Lynx. ☐ Other ______________	Ver: ___________ ☐ Yes ☐ No Ver: ___________ ☐ Yes ☐ No Ver: ___________ ☐ Yes ☐ No Ver: ___________ ☐ Yes ☐ No Ver: ___________ ☐ Yes ☐ No	☐ ________________ ☐ ________________ ☐ ________________ ☐ ________________ ☐ ________________ ☐ ________________	Ver:_________ ☐ Yes ☐ No Ver:_________ ☐ Yes ☐ No Ver:_________ ☐ Yes ☐ No Ver:_________ ☐ Yes ☐ No Ver:_________ ☐ Yes ☐ No Ver:_________ ☐ Yes ☐ No

Comments: ____

____

____

____

____

____

____

____

____

8.18 Audit Disaster Recovery Plan Process

While dry runs are indispensable for testing a disaster recovery plan, by their nature they are not comprehensive because they do not exercise every contingency in the plan. A disaster recovery audit, by contrast, attempts to check all the contingencies. An audit doesn't have the training value of a disaster recovery exercise, but it should provide a broader check of the plan's workability and value. This is particularly important when you have an outside vendor in the picture, because you want to make sure the outside vendor is properly backed up and secured.

The mission of ENTERPRISE's Business Continuity Program is to establish and support an on-going contingency planning program to evaluate the impact of significant events that may adversely affect customers, assets, or employees. This program is designed to ensure that ENTERPRISE can recover its mission critical functions, meeting its fiduciary responsibility to its stakeholders and complying with the requirements of the Securities and Exchange Commission (SEC), and other mandated requirements. ENTERPRISE has developed detailed Business Continuity Plans and Disaster Recovery Plans for the restoration of critical processes and operations. ENTERPRISE has dedicated resources to its contingency planning and disaster recovery program. Key features of this process include:

- Employee safety strategies and communications
- Systems and telecommunications accessibility
- Alternate physical site location and preparedness
- System backup and recovery

The audit process focuses on the guidelines, which incorporate industry best practices, for critical business units including

- Business Impact Analysis
- Business Continuity and Disaster Recovery Plans
    - Identifies time sensitive, mission critical processes' recovery time objectives (RTO) and business impacts.
    - .Updates and tests its business continuity and disaster recovery plans to support the business needs.
    - Reviews crisis management processes, employee communication vehicles, alternate site requirements, recovery management, and site-specific checklists.
- Work Area Recovery Strategy
- Testing processes (in accordance with regulatory requirements)
- Executive Management and Board of Directory Communication

ENTERPRISE
Vendor Disaster Recovery Planning Questionnaire

DRP and Business Continuity Strategy

1 In the event of a disaster or significant disruption, does your organization have documented plans for business continuity and IT disaster recovery? (NOTICE: *if your firm has no plan in place and has not intention of implementing a plan then your firm should be aware that our vendor / partnership relationship is subject to cancellation*)

Yes ________ or No ________

2 What type of failure scenarios or outages do you plan for?

____
____
____

3 What duration of time is assumed for each type of failure scenario or outage you plan for?

___________________________(please specify # and hours, days, weeks, months, etc. for each type)

4 Does the plan establish critical business functions with recovery priorities?

Yes ________ or No ________

5 If you answered "Yes" to Question (4), what is the expected recovery time for your critical business functions?

0 – 4 hours _____
4 – 8 hours _____
Within one day _____
1 – 2 days _____
More than 2 days _____
Other (please specify) _____
N/A _____

6 Does the plan account for interdependencies both internal and external to your organization?

Yes ________ or No ________

Team Responsibilities

When notified by the Emergency Management Team that the Disaster Recovery Plan and Business Resumption Plan (BRP) has been activated, the primary responsibilities of the team will be to use their resources to support the corporate recovery effort and to activate their Recovery procedures.

Team Leader Responsibilities / Checklist

Read the entire section before performing any assignments.

General

The Primary responsibility of the Team Leader is to provide *leadership* of the recovery team and coordinate support for the recovery effort. Other responsibilities include:

1. Participate in Resumption meetings with the Emergency Management Team.
2. Direct the Business Continuity efforts of your team.
3. Oversee communications activities of the team.
4. Coordinate with the Emergency Operations Center regarding all administrative issues.

Critical Functions

Restore the following critical functions:

RTO* Critical Function

_______ ____

* Recovery Time Objective (Amount of down time before outage threatens the survival of the ENTERPRISE. RTO is determined by Senior Executives)

8.23 Business Pandemic Planning Checklist

Plan for the impact of a pandemic on your business

Tasks	Not Started	In Progress	Completed
Identify a pandemic coordinator and/or team with defined roles and responsibilities for preparedness and response planning. The planning process should include input from labor representatives.	●	●	●
Identify essential employees and other critical inputs (e.g. raw materials, suppliers, sub-contractor services/ products, and logistics) required to maintain business operations by location and function during a pandemic.	●	●	●
Train and prepare ancillary workforce (e.g. contractors, employees in other job titles/descriptions, retirees).	●	●	●
Develop and plan for scenarios likely to result in an increase or decrease in demand for your products and/or services during a pandemic (e.g. effect of restriction on mass gatherings, need for hygiene supplies).	●	●	●
Determine potential impact of a pandemic on company business financials using multiple possible scenarios that affect different product lines and/or production sites.	●	●	●
Determine potential impact of a pandemic on business-related domestic and international travel (e.g. quarantines, border closures).	●	●	●
Find up-to-date, reliable pandemic information from community public health, emergency management, and other sources and make sustainable links.	●	●	●
Establish an emergency communications plan and revise periodically. This plan includes identification of key contacts (with back-ups), chain of communications (including suppliers and customers), and processes for tracking and communicating business and employee status.	●	●	●
Implement an exercise/drill to test your plan, and revise periodically.	●	●	●

9.0 Change History

Version 8.0 – Released March 2014

- Updated to be compliant with the latest ISO standards
  - Added section on ISO 28000
- Updated to the latest Business and IT Impact forms (Now included as a separate document for ease of use)
- Updated to include specific references to mobile users and BYOD devices
- BYOD back up recovery strategy before and during a disaster defined
- Updated with the latest electronic forms
- Updated with the latest Business Impact and Risk Assessment

Version 7.5 – Released June 2013

- Added Physical and Virtual Server Security Policy
- Added Electronic Form
  - Server Registration

Version 7.4 – Released February 2013

- Updated Recovery Site Strategy for Cloud
- Updated CSS Style Sheet for black and white printing
- Corrected minor errata

Version 7.3 - Released September 2012

- Updated the included files to include Version 1.3 of the Disaster Recovery Business Continuity Audit Program

Version 7.2 - Released March 2012

- Updated responsibilities for team members
- Added Safety Program references in the core template
- Added Electronic Safety Program Forms
  - Area Safety Inspection
  - Employee Job Hazard Analysis
  - First Report of Injury
  - Inspection Checklist – Alternative Locations
  - Inspection Checklist – Office Locations
  - New Employee Safety Checklist
  - Safety Program Contact List
  - Training Record

Version History

Version 7.1 - Released January 2012

- Updated graphics
- Updated Business Analysis Impact Section

Version 7.0

- Updated for compliance with ISO 22301
- Added Electronic Forms for Disaster Recovery and Business Continuity Plan Management
  - Plan Distribution Control Log
  - Remote Location Contact Information
  - Team Call List
  - Vendor Contact List
  - Off-Site Inventory
  - LAN Hardware / Software Inventory
  - Personnel Locations

Version 6.2

- Added ISO 27031 specific materials
  - Overview
  - Principles – Scope and Objectives
  - Requirements

Version 6.1

- Added materials specific to social network communication
- Added Social network checklist

Version 6.0

- Updated Disaster Recovery Audit Program for mandated requirements
- Updated Business & IT Impact Questionnaire for mandated requirements
- Updated backup strategy section
- Added Incident Communication Plan

Version 5.7

- Updated Communication Strategy and Policy
  - Added Communicating with employees section
  - Added What to communicate section

Version History

Version 5.6

- Updated Business and IT Impact Questionnaire
  - Updated for COBIT compliance
  - Updated for PCI-DSS compliance
  - Updated for US state level compliance (New York, Massachusetts, and California)
  - Update for ISO security requirements

Version 5.5

- Updated to comply with CobiT requirements
- Sample Disaster Recovery Plan Service Agreement

Version 5.4

- Added Pandemic Coordinator job description
- Added Business Pandemic Planning Checklist
- Updated organization chart to include Pandemic Coordinator
- Corrected minor errata

Version 5.3

- Updated backup and backup retention section
- Updated style sheet to be CSS Style sheet format
- Added Disaster Recovery Business Continuity General Distribution Information
  - What to do after an explosion / terrorist attack
  - How to clean up after a disaster

Version 5.2

- Updated style sheet to WORD 2007 format
- Updated forms and charts

Version 5.1

- Added sample Backup and Backup Retention Policy
- Minor formatting changes

Version 5.0

- Updated Disaster Recovery / Business Continuity Plan Audit Program to be compliant with ISO 27000 Series (ISO 27001 and ISO 27002)
- Added a section on Communication Strategy and Policy to be implemented when the Disaster Recovery / Business Continuity Plan is activated
- Added a section on Disaster Recovery / Business Continuity and Security basics
- Added Personnel Location Report
- Added Project Status Report Form

Version History

Version 4.5

- Added Disaster Recovery / Business Continuity Plan Audit Program
- Updated excel work plan to refer to sections versus pages

Version 4.4

- Section added on implications of Sarbanes-Oxley, Treadway Commission, and PCI DSS requirements
- Disaster Planning Branch Offices added
- Backup strategy table added
- Backup strategy for PDA's updated to reflect Smartphones

Version 4.3

- Defined generic metrics for DR/BC success
- Business & IT Impact Analysis Questionnaire Updated
- Updated references to DRP card
- Updated formatting to meet WORD 2007 requirements

Version 4.2

- Added Section defining the ISO 17799 compliance requirements
- Review and modified entire DRP/BCP template to ensure compliance with ISO 17799
- Business & IT Impact Questionnaire updated to meet ISO 17799 compliance requirements
- Corrected errata
- Added Best Data Retention and Destruction Practices Section

Version 4.1

- Department DRP / BCP Activation Workbook Updated in the appendix
- Correct work plan formatting and numbering for project initiation
- Web Site Disaster Recovery Planning Form added to the appendix

Version 4.0

- Vendor Disaster Recovery Planning Questionnaire added to the appendix
- Department Disaster Recovery Planning Workbook added to the appendix
- Vendor Phone List form updated
- Key Customer Notification List form added
- Critical Resources to be Retrieved form added
- Business Continuity Off-Site Materials form added

Version History

Version 3.1

- Site Strategy section added (Section 3.1) all other section numbers in Chapter 3 were increased to adjust for this modification.
- Audit Disaster Recovery Plan Process added (Section 8.13)
- Manager Disaster Recovery and Business Continuity job description added
- Entire template reviewed to validate compliance with Sarbanes-Oxley