To use the links, please extract all of the files in this .Zip archive. The tools work best from the same folder as this PDF.

IT Continuity Planning: Business Impact and Risk Assessment

Bundle 1: Step-by-Step

Step 1: Assess Threats and Risks

The first task in completing your IT Continuity Plan is having a clear idea of how IT assets are vulnerable to threats and what level of protection you have in place. This means you need to know what assets you have, the specific risks to those assets, and what steps you have taken to secure them.

Info-Tech Tip: These steps are critical for any company developing a DRP. The tools suggested are designed to support these steps for organizations with any number of IT assets and associated risk.

1.1 Inventory Corporate Assets

Use these Tools and Templates:

Corporate Asset Inventory

1.2 Identify Threats/Risks Specific to Assets

Use these Tools and Templates:

Potential Risk Checklist

1.3 Identify Existing Mitigation

Use these Tools and Templates:

DRP Operational Analysis

1.4 Summarize the Operational Analysis

Use these Tools and Templates:

Operational Analysis Summary

Step 2: Assess Data Center Vulnerabilities

Given that most of the IT assets of any organization reside within the all-important data center, it is crucial to conduct an audit of the data center and to assess the probability of a disaster (or a security breach) occurring in this area.

Info-Tech Tip: In addition to identifying areas of weakness for the DRP, an audit of the data center provides a general assessment of data center security that can be provided to external auditors for compliance.

2.1 Conduct An Audit of the Data Center

Use these Tools and Templates:

1. Data Center Security Audit

2. Data Center Security Audit (Core)

2.2 Conduct Probability Assessments

Use these Tools and Templates:

Data Center Risk Probabilities

Step 3: Confirm DRP/Business Context

This step is comprised of only a single task, using two tools to document important information. Documenting key stakeholders at this point is important in order to get everyone on board once risks and business impact have been identified for corporate assets. This allows you to come to the table with some DRP information already complete.

Info-Tech Tip: Using the DRP workbook provides you with an opportunity to hone your communication skills when conversing with business managers and other stakeholders. Be sure to clearly outline what you hope to achieve in your discussions with them.

3.1 Document Business Structure and Key Stakeholders

Use these Tools and Templates:

1. Disaster Recovery Planning Workbook

2. Call Tree

Step 4: Assign Value to IT Assets

Before the enterprise spends any budget dollars on a DRP, IT must first work with various business units to determine the actual value of the assets that need protection. After all, no one would spend $1 million to protect an asset that is only worth $50,000 (including loss of revenue due to downtime of the asset and other factors).

Info-Tech Tip: Completing these tools will assist you in defining the value of your assets, and will also demonstrate to upper management the need for additional funding to protect the most critical aspects of the DRP.

4.1 Plan Against Downtime/Loss of Asset

Use these Tools and Templates:

Downtime Policy

4.2 Conduct a Business Impact Analysis

Use these Tools and Templates:

Risk and Business Impact Analysis Worksheet

Technical Risk Analysis Report

Step 5: Assign Prioritization to Assets

Once threats to assets have been identified, probabilities determined, and the cost of threats estimated, it is time to prioritize which assets must be brought back online first in the event of a disaster.

Info-Tech Tip: You are strongly encouraged to complete these steps and their corresponding tools, as they (along with the business impact analysis from Step 4) will form the heart of your DRP.

5.1 Prioritize Recovery by Impact to Business Units

Use these Tools and Templates:

Business unit Prioritization

5.2 Document Prioritized Recovery List

Use these Tools and Templates:

Recovery Prioritization Meeting

Step 6: Determine Costs vs. Risk Tradeoff

Now that you know which assets are critical and the steps required to improve resiliency, there is still the task of justifying those efforts through return on investment (ROI) calculations. Offsite DRP efforts are treated separately here because of the elevated costs of building a hot site or cold site to house redundant servers, storage, desktops, and so on.

Info-Tech Tip: Bear in mind that this step is for discovering the ROI of fixing vulnerabilities that currently exist in the organization, not for the DRP project itself.

6.1 Conduct ROI Studies

Use these Tools and Templates:

1. Migration Project ROI& Prioritization Tool

2. Return on Security Investment Calculator

Step 7: Maintain Risk Plans

In order for the to DRP to execute as expected, risk plans must be maintained and kept current, particularly as the company grows, which can change its threat profile. In order to keep risk plans and profiles current, two tasks must be carried out.

Info-Tech Tip: Larger companies may need to spend more time on their risk reports and tracking, as more complex infrastructures have a greater number of assets, and therefore higher risk. For smaller companies, the risk management process does not have to be an onerous one. Therefore, please use these tools accordingly.

7.1 Create Asset-Specific Risk Reports

Use these Tools and Templates:

Asset Risk report

7.2 Document, Track, and Manage Risks

Use these Tools and Templates:

Risk Management Spreadsheet