

DAP

Data Asset Protection Planning



Risk Assessment and Business Continuity Planning Guide

Major Concept:

Business
Continuity:
Protection
detection, and
response planning
to prevent attacks
against your
digital assets

Primary Issue:

Protecting
mission critical
assets and
processes

Key Business Strategy:
Proactive planning
using controls and
technology to
prevent the loss of
digital assets



STELZL VISIONARY LEARNING CONCEPTS

Emerging Market Business Strategies

© Stelzl Visionary Learning Concepts
7608 Big Buck Trail, Waxhaw NC
Phone 704.243.0014 • Fax 704.243.0867

Digital Asset Protection Planning Process, Rev 2.1

Copyright © 2004 by Stelzl Visionary Learning Concepts, Inc.

All rights reserved

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means – electronic, mechanical, photocopying, recording, or otherwise-without written permission from Stelzl Visionary Learning Concepts, Inc.

Assessing Business Continuity

Business continuity is the most important plan issue facing businesses today. The importance is largely centered on information technology because 90% of a company's information is digital. During the last five years we have seen a growth trend in data compounding at sixty (60) percent per year. In order to ensure that your business remains healthy through a difficult and unforeseen interruption, it is of paramount importance to have a robust business continuance plan that is thorough, supported by the executive management and clearly understood by everyone in the organization. In this document we assess each area that is essential to successful business continuance in an unforeseen event. These areas include the following:

Quote:

70% of businesses that have a major disaster or business interruption go out of business within two years.

Areas to consider:

Governance:

Risk analysis:

Business impact analysis:

Information storage analysis:

DR plan assessment:

Strategy:

Understand your organization's critical assets, uncover relevant threats, and assess your ability to reduce or stop the impact of an unexpected event which threatens these assets.

Important terms

Business continuity	Business continuity planning is a strategy to minimize the affect of disturbances and to allow for the resumption of business processes.
Disaster recovery	Disaster recovery is the capability to implement critical processes at an alternative site and to return to the primary site and normal processing within a time frame that minimizes the loss to the organization, by executing rapid recovery procedures.
MTD	The Maximum Tolerable Downtime that a business can tolerate and still remain a viable company; that is, what is the longest period of time a critical process can remain interrupted before the company can never recover.
RTO	Recovery Time Objective is the time required recovering critical business systems to a functional state from the occurrence of a disruption.
RPO	Recovery Point Objective is the point in time, preceding the interruption, that data must be available to allow the business functions to resume operations.
Asymmetric vs. symmetric	Asymmetric vs. symmetric: In data management, a symmetric commit requires that data must be written to each copy area before it is accepted by a storage array. Asymmetric commits allow time to pass before the second copy of the data is committed.
Hot site	A hot site is a disaster recovery alternative back-up site that is a fully configured computer facility with electrical power, heating, ventilation and A/C and functioning file/print servers and workstations. Applications that are needed to sustain remote transaction processing are installed on servers and workstations and are kept up to date to mirror the production system.
Warm site	A warm site is a computer facility readily available with electrical power, A/C and computers but the applications may not be installed or configured. It might have a subset of file/print servers and workstations. External communication links and other data elements will be installed.
Cold site	Cold site is a room with electrical power and HVAC but all hardware (file/print servers, workstations) and application will need to be installed and current data restored from backups.
Traditional recovery	Tape back-up of production data, tapes are sent off-site, stored and sent to a warm site for disaster recovery.
Advanced recovery	A recovery solution which provides a recovery time and recovery point objective that is less than a traditional warm site solution.

Process Overview

The purpose of this effort is to provide an executive level overview of the client's business continuity and disaster recovery requirements, drawing conclusions, actions and recommendations for our client.

We will be meeting with your key personnel to examine the variables in each defined area listed in the *Areas to consider* table. This assessment is designed to be completed in one day, with the actions and recommendations to be delivered within a week.



As the above diagram shows there are three steps to our process.

1. The first is meeting with key individuals to examine the areas described above. Concurrently we will use software to determine the usage patterns of your IT servers and data storage.
2. The second step is the analysis and compilation of the information into a useful format.
3. The third step is the presentation of those items that appear problematic and assigning the corrective actions to responsible individuals or teams.

IMPORTANT PRIORITY:

The number-one priority of all business continuity and disaster recovery planning is “people first”. While we talk about the preservation of capital, resumption of normal business processing activities and other business continuity issues, the main overriding concern of all plans is to get the personnel out of harm’s way. Personnel evacuation and safety must be the first element of a disaster response plan. “Krutz and Vines CISSP Prep Guide”

Step 1: Understanding Governance

Corporate governance refers to the manner in which a corporation is directed. It includes the laws governing the formation of firms, the bylaws established by the firm itself, and the structure of the firm. The corporate governance structure specifies the relations and the distribution of rights and responsibilities, among primarily three groups of participants – the board of directors, managers, and shareholders. This system spells out the rules and procedures for making decisions on corporate affairs; it also provides the structure through which the company objectives are set, as well as the means of attaining and monitoring the performance those objectives. The fundamental concern of corporate governance is to ensure the conditions whereby a firm's directors and managers act in the interests of the firm and its shareholders, and to ensure the means by which managers are held accountable to capital providers for the use of assets.



IT Governance:

Governance and asset protection require a high-level commitment to the information security policy process. Managers must understand how important security controls and protections are to the enterprise's continuity.

Governance Ensures that senior management understands and supports the criticality of digital information to the health and welfare of the enterprise.

Governance uses policies and standards to drive architecture, which in turn will guide designs and IT practices.

Strategy:

Use security policies to create specific technology standards and to develop detailed procedures. Use technology to managed

Policy hierarchy

Charter Policy	The Senior Management Statement of Policy or Charter Policy includes: (1) an acknowledgement of the importance of the computing resources to the business model (2) a statement of support for information security throughout the enterprise and (3) a commitment to authorize and manage the definition of the lower level standards, procedures and guidelines.
Regulatory Policies	Regulatory policies are security policies that an organization must implement due to compliance, regulation or other legal requirements.
Advisory Policies	Advisory policies are policies that are not mandated to be followed but strongly advised
Informative Policies	Informative policies are those that exist simply to inform the reader
Standards	Standards are driven by corporate information security policies and specify the use of specific technologies in a unified way
Guidelines	Recommended actions, not compulsory
Procedures	The detailed steps that are followed to perform a specific task.
	Notes:

Policy Structure

Charter Policy	The Information Security Program Charter serves as the capstone document for the Information Security Program and empowers the Information Security Program to manage Information Security-related business risks.
Asset identification & classification	The Asset Identification and Classification Policy defines objectives for establishing specific standards to define, identify, classify, and label information assets.
Asset protection	The Asset Protection Policy defines objectives for establishing specific standards for providing an appropriate degree of confidentiality, integrity, and availability for information assets.
Asset Management	The Asset Management Policy defines objectives for properly managing Information Technology infrastructure, including networks, systems, and applications that store, process and transmit information assets throughout the entire life cycle.
Acceptable use	The Acceptable Use Policy defines objectives for ensuring the appropriate business use of information assets.
Vulnerability assessment and management	The Vulnerability Assessment and Management Policy defines objectives for vulnerability assessment activities and ongoing vulnerability management efforts.
Threat assessment and monitoring	The Threat Assessment and Monitoring Policy defines objectives for threat assessment activities and ongoing threat monitoring efforts.
Security awareness	The Security Awareness Policy defines objectives for establishing a formal Security Awareness Program.
	Notes:

Step 1. Do you have a security policy (Is it accessible to all employees, maintained with regularity, and signed off on by each employee)?

Step 2. Is there a process to classify digital assets as they are created (classification is related to the DR and BCP because both focus on business risk and data valuation)?

Step 3. How are end-users trained on policy and security awareness? Do they understand what a security violation is and how one occurs?

Are they willing to take action - why?

What is the protocol to follow in the event of a policy violation?
