

Disaster Recovery Readiness: Policy Design and Implementation

Highlights:

1. A transformative approach to disaster recovery policy design and implementation.
2. Clearly defined and documented disaster recovery policies that map to specific corporate goals and accepted by key stakeholders.
3. Confidence that your disaster recovery capabilities meet your current needs with flexibility for growth and improvement.

Getting business continuity and disaster recovery right is a big challenge. An organization must understand the risks it faces and how different systems and approaches create an optimal level of protection.

Bob Laliberte
Enterprise Strategy Group

Offering Summary

Data loss, degraded business operations in disaster situations, and failure to pass corporate disaster recovery (DR) audits can be costly to you and your company. In addition to the direct monetary costs, today's poor DR design can have a significant impact on your reputation and industry position if a disaster recovery situation is declared.

One of the key challenges with designing a modern disaster recovery environment is that today's applications extend beyond physical server, virtual server, and even datacenter boundaries. CommVault helps its clients overcome these challenges by working closely with them during a facilitated workshop session to build a business aligned, multi-site DR architecture and implementation plan. CommVault can then execute the implementation plan to put the proposed architecture in place.

During the workshop with client stakeholders, CommVault professionals assess their legacy DR approaches, as well as their Recovery Point Objectives, Recovery Time Objectives, and other important business requirements. Then, CommVault consultants use these inputs as a foundation for executive level advice that transforms their traditional operations into standards for disaster recovery readiness. Finally, clients may choose to extend the design engagement into delivery and implementation activities. Here they can leverage the experience of hundreds of trusted CommVault Services professionals to achieve that standard quickly and cost effectively.

CommVault's comprehensive, customer-centric approach to designing and implementing disaster recovery environments brings confidence to clients because their unique business requirements have been incorporated from the beginning. Should a disaster strike, our clients can rest assured that any underlying Simpana[®] software implementation has been installed and configured in strict alignment with corporate goals for recovery.

Disaster Recovery Design

CommVault employs standard methodologies, best practices, and the in-depth expertise of a dedicated team of consultants, architects, engineers, and industry experts to deliver its **Disaster Recovery Readiness and Policy Design** offering. The CommVault team works closely with the client's IT and business leaders to discover the current state of their recovery environment, create a vision for modern, yet pragmatic capabilities, develop design alternatives, make recommendations for optimal disaster recovery policies, and propose architectures and configurations that meet those needs. Clients can expect to participate in the following activities over the life of an engagement:

Set Priorities – Identify and document corporate goals and key business drivers that will define disaster recovery requirements

Policy Development – Develop strategic, tactical and operational policies that help define the overall disaster recovery program

Define DR Requirements by Application – Conduct an application recovery requirements analysis to determine which applications are most critical and priority for recovery.

Recovery Service Catalog – Define concrete Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for applications and associated data

Recommended Architecture – Design a high level architecture that meets the discrete recovery service levels identified in the Recovery Service Catalog

Remediation Planning – Assess IT Infrastructure readiness and build a remediation plan for IT utility components like: VPN concentrators, DNS, Active Directory (AD), data protection, firewalls and other tier-zero applications.

Site Planning – Assess site recovery readiness and develop plans that ensure primary and DR sites can support a DR capability. This includes discussions on insourcing, outsourcing, cloud, and cross site recovery strategies.

Disaster Recovery Implementation

A **Disaster Recovery Readiness and Policy Implementation** engagement typically follows policy design. CommVault engineers use the results of the policy design to develop and execute a detailed action plan that includes installation, configuration, and hand-off of the Simpana software disaster recovery environment in accordance with architectural design recommendations. The implementation effort is broken up into three steps:

Technical Design

Detailed specifications and infrastructure schematics are generated that conform to the future state or “to be” architecture. These support the tiered recovery service policies enabled by Simpana software. The results of technical design are captured in a master document which contains these key elements:

- Overview of major work streams and dependencies in a precedence diagram format
- Level-of-effort estimates for each work stream
- Detailed project plan with assigned resources, milestones, and estimated time to completion
- Check list of required infrastructure for the build phase

Build

In this step, CommVault provides implementation specialists that configure the IT environment as it is defined in the technical design master document. CommVault engineers work with you to deploy and configure Simpana software in your environment, thereby accelerating your time to value and reducing your risk in the event of a disaster.

The Policy Implementation offering can be applied to the redesign of an existing Simpana software environment, as well as a new CommVault customer environment. Engineers ensure that the environment is configured in accordance with industry leading practices and is optimized for each client’s unique operating design requirements.

Transition

CommVault documents and builds a training plan specific to the customer’s future state environment. The goal is to create a smooth transition from initial start-up to a steady-state, internally managed and tiered DR capability. Transition to the customer includes all documentation and artifacts, solution specific product training, and industry leading support services.

Key Service Components and Benefits



Component	Benefits
Standard Delivery Approach	CommVault consultants and the knowledge base supporting them leverage years of industry experience and thousands of unique data protection and recovery customers. Their skill and expertise is incorporated into a facilitated workshop approach that dramatically reduces design time and implementation execution.
Disaster Recovery Design	The Disaster Recovery Readiness and Policy Design engagement includes input and direction from the customer's key stakeholders who are responsible for ensuring that critical business functions continue in the event of a disaster. Their direction is incorporated into a tiered disaster recovery design that is balanced among cost, risk, and quality of service requirements.
Disaster Recovery Implementation	Key service level attributes of the design engagement are implemented through the Simpana [®] software platform by CommVault's experienced engineers. These implementation steps ensure that business requirements for the disaster recovery plan are properly incorporated into the Simpana configuration and result in a reliable, cost effective tiered recovery environment.
Prioritized Policies	CommVault disaster recovery specialists work with the client to build a prioritized list of strategic, tactical, and operational policies that define the official corporate position for response to disaster recovery situations.
Business Aligned Disaster Recovery	Key business functions and applications are identified along with respective needs for business resiliency. These requirements are the basis for building recovery capabilities that are in-line with their business value.
Recovery Service Catalog	Disaster recovery service attributes such as RTO and RPO are captured in a tiered recovery service catalog that is the centerpiece for providing disaster recovery as a service. The catalog is a vital element for building service level attributes that are easily incorporated into Service Level Objectives (SLO) or Service Level Agreement (SLA) documentation.

For more information about CommVault Simpana[®] software and services please visit <http://www.commvault.com/>



www.commvault.com • 888.746.3849 • E-mail: info@commvault.com

CommVault Worldwide Headquarters • 2 Crescent Place • Oceanport, NJ 07757
Phone: 888-746-3849 • Fax: 732-870-4525

CommVault Regional Offices:
United States • Europe • Middle East & Africa • Asia-Pacific • Latin America & Caribbean • Canada • India • Oceania