redesign

redesign-group.com

SERVICE BRIEF

Dell Cyber Recovery
Vault Audit

re

This document outlines the scope, deliverables, responsibilities, and terms governing Redesign's Dell Cyber Recovery Vault Audit Services. This engagement evaluates the configuration, resilience, and operational readiness of Dell's Cyber Recovery Vault implementation, ensuring it aligns with Dell best practices and industry standards for cyber resilience and ransomware recovery.

This engagement is governed by this Service Brief and associated with SKU: SEC-DELL-VAULT-AUDIT.

The quantity defined in the quote reflects the number of Dell Cyber Recovery Vaults to be audited.

The *future* belongs to the *curious*.

Table of Contents

01. Services Overview

Redesign's Dell Cyber Recovery Vault Audit is designed to assess the integrity and effectiveness of Dell's Cyber Recovery solution, including the vault's air gap configuration, access controls, recovery procedures, and governance. This engagement provides a point-in-time analysis of the customer's cyber recovery readiness, helping identify gaps that may impact the organization's ability to recover from ransomware or destructive cyber events.

02. Offer Structure

PRIMARY SERVICES

- Audit of the Dell Cyber Recovery Vault architecture and configuration
- Evaluation of vault air-gap implementation and Secure Copy procedures
- Review of retention, immutability, and replication settings
- Analysis of access controls and CyberSense integration
- Comparison against Dell Cyber Recovery Solution best practices

OPTIONAL ADD-ONS

Separate SOW

- Remediation and configuration support
- Cyber Recovery Plan creation
- Integration with IR tabletop or business continuity testing
- CyberSense optimization review

03. Project Scope

This engagement includes a technical and procedural audit of the Customer's Dell Cyber Recovery Vault environment, including associated Data Domain systems, Cyber Recovery software, and CyberSense deployment. The audit will evaluate the vault's architecture, separation from production, integrity protections, administrative procedures, and readiness to support ransomware recovery.

All devices must be functional, supported, and reachable for inclusion.

04. Quantity & Effort Model

- **Service SKU: SEC-DELL-VAULT-AUDIT**
- **Quantity: Number of Dell Cyber Recovery Vault environments to be assessed**
- **Work per Unit Includes:**
  - One discovery and architeture review
  - One written findings and recomendation report

MONTHLY SUPPORT TERMS

This service includes up to the number of hours specified in the associated quote for operational support per month, limited to the activities defined in this Service Brief.

Unused hours do not carry over to subsequent months. Additional support hours may require a revised quote or a separate Statement of Work (SOW).

05. Services & Key Activities

Stage	Key Activities
Discovery & Documentation Review	▪ Conduct kickoff meeting and scope validation ▪ Review vault architecture, policies, and runbooks ▪ Identify Data Domain replication strategy, Cyber Recovery software version, and policy settings ▪ Collect vault access logs and backup workflow documentation
Vault Configuration & Controls Review	▪ Validate air-gap logic and Secure Copy configurations ▪ Assess logical and physical separation from production ▪ Review Cyber Recovery policies, immutability, and retention settings ▪ Evaluate administrative access controls and change management workflows ▪ Assess CyberSense configuration and alert tuning
Risk Analysis & Recommendations	▪ Identify configuration drift or security exposures ▪ Prioritize findings and offer remediations ▪ Deliver executive and technical summaries

06. Deliverables

Dell Cyber Recovery Vault Audit Report

Knowledge Transfer (virtual, 1 hour)

07. Services Scope Changes

Auditing multiple vaults, conducting recovery simulations, or implementing configuration remediations may require a revised quote or change order.

---

08. Services Scope Exclusions

This engagement does not include:

- **Live incident response or active ransomware recovery**
- **Reconfiguration of the vault or underlying systems**
- **Licensing or provisioning of Dell software/hardware**
- **CyberSense installation or patching**
- **Network segmentation or production environment testing**

09. Customer Responsibilities

- **Assign a technical point of contact familiar with the vault**
- **Provide remote access to Dell Cyber Recovery Vault and associared components**
- **Share current documentation for recovery workflows and vault SOPs**
- **Ensure any required remote access is available or approved**

Failure to meet these requirements will prevent Redesign from delivering the services outlined in this Service Brief.

10. Services Schedule

- **Start Date:** Upon signed quote and kickoff
- **Completion:** Project signoff via DocuSign by customer

---

11. Terms and Conditions

This engagement will be governed by the Seller's terms and conditions located at:

- www.redesign-group.com/legal

ONSITE SERVICES WILL NOT BEGIN UNTIL THE FOLLOWING PREREQUISITES ARE MET

- Signed quote referencing SKU: SEC-DELL-VAULT-AUDIT and quantity
- Remote Vault access approved or documentation provided
- Stakeholders assigned and kickoff scheduled

Failure to meet these requirements will prevent Redesign from delivering the services outlined in this Service Brief.

redesign

The *future* belongs
to the *curious*.

↗ redesign-group.com