

SHIELDRecovery Product Suite



INTENT

CTI's SHIELD Disaster Recovery (SHIELDRecovery) suite is intended to provide organizations with business / IT system continuity and disaster recovery planning, disaster recovery design and testing, and all associated documentation. The purpose of this suite is to assist in development of documentation that validates the organization's system recovery and continuity expectations, and establish the necessary processes and procedures to meet those goals. The three (3) assessments comprising the SHIELDRecovery suite provide varying degrees of planning, review, testing, and documentation suitable for diverse needs and budgets. Recommendations for new solutions or additional functionality will assist in determining the timeliness of successful recovery.

COMPONENTS

The following graphic illustrates the various assessments available as part of CTI's SHIELDRecovery suite. These services range from concise one- to three-day engagements to detailed multi-week assessments.

SHIELDRecovery Express

Have that one critical business application or service that you could not afford to be without? CTI's SHIELDRecovery Express will ensure that critical applications can be recovered with minimal downtime and data loss. This test includes a full recovery scenario, which will be documented to allow any user to recover the application following a disaster or disruption. This assessment requires minimal customer involvement, reducing the impact on day-to-day business.

SHIELDRecovery Core

SHIELDRecovery Core blends disaster recovery design and assessment. With the Core offering, you are able to test and recover up to eight (8) applications at three (3) locations. In addition, a Disaster Recovery Plan (DRP) will be designed and tailored to fit your organization's need and overall strategy. In-depth scanning and personnel interviews will be conducted to ensure all information is gathered and documented. The creation of the DRP will prepare and assist the organization to recover from a variety of disaster scenarios.

SHIELDRecovery Pro

SHIELDRecovery Pro is CTI's most comprehensive Disaster Recovery offering. Founded on recovery best practices and industry experience, this assessment will produce a detailed IT Availability and Disaster Recovery solution built from the ground up to fit your organization's recovery needs. Critical business applications at all of your locations can be tested with multiple disaster scenarios to provide thorough outcomes and reporting. Network documentation will also be created to visualize network device connectivity and communication links.

SECURITY HEALTHCHECKS | INTERNAL EVALUATIONS | LOGISTICAL DOCUMENTATION

BREAKDOWN

	SHIELDRecovery Express	SHIELDRecovery Core	SHIELDRecovery Pro
Appropriate for review by regulatory auditors?	Yes	Yes	Yes
Level of customer participation required?	Minimal	Moderate	Significant
IT Leadership and Network Interviews?	No	Yes	Yes
Pre-Test Health Check?	Yes	Yes	Yes
Number of Locations?	1	2-3	4+
Number of Critical Business Applications to Test?	1-3	4-8	9+
Number of Recovery Scenarios to Test?	1	2-3	4+
Review of Disaster Recovery Policies and Procedures?	No	Yes	Yes
Creation of Business Continuity and/or Disaster Recovery Plan?	No	Yes	Yes
Creation of IT Availability Risk and DR Solution Design?	No	No	Yes
Level of Automated Scanning?	No	System and Application Inventory Scanning	System and Application Inventory Scanning
Systems Information Gathering?	No	Yes	Yes
Application Dependency Documentation?	No	Yes	Yes
Creation of Network Documentation?	No	No	Yes
CTI Supplied Disaster Recovery Equipment?	Yes	Yes	Yes
Documentation of Recovery Procedures?	Yes	Yes	Yes
Recommendations for Improvement?	Yes	Yes	Yes
Applicable regulatory standards?	HIPAA, GLBA, FFIEC, HITRUST, etc.	HIPAA, GLBA, FFIEC, HITRUST, etc.	HIPAA, GLBA, FFIEC, HITRUST, etc.
Average assessment duration?	1-2 days	5-7 days	2-3 weeks
Delivery meeting included?	Yes	Yes	Yes

SELECTION

Answers to the following questions will help determine which level of service your organization should select:

- 1) Approximately how many servers do you have in your environment? (Virtual and/or Physical)
- 2) About how many business units (departments) are in your organization?
- 3) Is your organization subject to any regulatory requirements?
- 4) How many physical office locations would be visited during this assessment?



SECURITY HEALTHCHECKS | INTERNAL EVALUATIONS | LOGISTICAL DOCUMENTATION