# Operational Resilience Checklist

## Essential considerations for achieving Physical System Recovery at scale.

www.cristie.com

# Introduction

System recovery is fundamental to achieving operational resilience for business services identified as critical. Despite the dominance of virtual and cloud computing, physical machines remain the essential infrastructure underpinning all enterprise applications.

Unfortunately, physical systems lack the automation of virtual environments, leading to time-consuming manual processes during recovery.  In addition, compatibility issues often arise due to the tight link between hardware and operating systems. Businesses rely heavily on physical servers, so any delay in their recovery can severely disrupt operations and hinder meeting service impact tolerances and recovery time objectives (RTO).

Critical business services must also be restored in a specific order to cater for application dependences. To achieve this the underlying system recovery solution will require orchestration features to allow for customization of the system recovery workflow. Firms that come under the scope of regulatory directives will need to perform regular testing of recovery plans under realistic disruption scenarios. Compliance efforts must also be thoroughly documented including the specific methods used during recovery testing.

This checklist document will outline eight key functional capabilities that should be present within any system recovery solution. These core capabilities will help to solve the challenges of physical system recovery at scale, orchestrate and automate disaster recovery scenario testing, and support self-assessment through detailed system recovery simulation and reporting.

# Operational Resilience System Recovery Checklist

## ✓ Automation for physical machine recovery at scale.

Your recovery solution should eliminate manual intervention from physical machine recovery and integrate with boot management tools (IPMI) to control the entire boot process. Support for automated dissimilar hardware recovery should also be included.

## ✓ Orchestration for staged application recovery.

Systems will need to be recovered in a specific sequence to ensure that all application dependencies are supported. Your recovery solution should provide sequenced recovery plus the ability to add pre- and post- boot operations.

## ✓ Recovery to an isolated test environment.

Having the ability to recover systems to an isolated network environment allows for activities such as pen testing, patch verification and cyber forensics, without posing any risk to the production environment.

## ✓ Advanced reporting for regulatory self-assessment.

Operational resilience regulations require demonstrated recovery of critical business operations through self-assessment. Your system recovery solution should provide detailed reporting on system recovery performance to support self-assessment requirements.

# Operational Resilience System Recovery Checklist

## ✓ Simulated recoveries for RTO & integrity verification.

The ability to schedule simulated recoveries enables the integrity of system recovery images to be verified and recovery time objectives (RTO) checked against critical application impact tolerances.

## ✓ Machine Learning driven recovery rectification.

The application of Machine Learning (ML) should play a key role in any modern system recovery solution. ML can provide self-healing capabilities to rectify common system recovery failure scenarios without manual intervention.

## ✓ Advanced Anomaly Detection.

Machine Learning can provide early warning of anomalies in file structure which may indicate malicious file encryption as a precursor to ransomware activity. Your recovery solution should include the capability to test recovery image integrity and detect abnormal file structure changes between subsequent backups.

## ✓ Test environment setup and reset.

The ability to quickly setup and reset a system recovery test environment is an important feature to reduce administrative overhead and minimize downtime following a cyber-attack or any other system outage scenario.

cristie
software

### *Where to find additional information & resources*

Cristie Software recovery solutions can overcome the challenges of physical system recovery at scale while providing complete flexibility to restore to and from any platform type.  Contact our team anytime sales@cristie.com to learn more about simplifying key aspects of infrastructure recovery to help meet the requirements of operational resilience legislation. Visit the System Recovery and CloneManager® product pages for more information regarding the Cristie Software suite of solutions for system recovery, replication, migration, and ransomware protection.

Cristie Software - Simplifying Operational Resilience - Online Resources

Cristie Software - System Recovery and Replication Use Cases