VERITAS

The Always-On, Always Ready Financial Institution

Strategies for ensuring high availability and operational resiliency

White Paper | June 2023

Contents

Introduction

Financial Services Institutions (FSIs) face an ever-increasing threat landscape. Regulators worldwide are adapting or introducing regulations to ensure these organizations remain operationally resilient, especially where they are considered critical to the nation's fabric. Boards and senior management's focus on their firm's operational resilience will become increasingly important as the wider financial sector becomes more dynamic, complex, and reliant on technology and third parties. Firms must set and meet precise standards for the services they provide, and test their ability to meet those standards.

The Basel Committee on Banking Supervision defines operational resilience as the ability of a bank to deliver critical operations through disruption. As such, banks must consider their overall risk appetite and tolerance for disruption, where tolerance is the level of disruption from any type of operational risk a bank is willing to accept, given a range of severe but possible scenarios. Critical operations include activities, processes, services, and supporting systems and assets where disruption would impact the bank's continued operation or its role in the financial system.

Building on the Basel Committee paper, operational resilience regulation continues to gain momentum around the world. For example, the European Commission (Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector), the UK Prudential Regulation Authority (Supervisory Statement SS1/21 Operational resilience: Impact tolerances for important business services), the US Federal Banking agencies (Sound Practices to Strengthen Operational Resilience) and the Hong Kong Monetary Authority (Supervisory Policy Manual Operational Resilience), to name a few, have all added their perspectives on this subject.

A strong theme throughout these regulations is for FSIs to build, operate, assure, and review their operational resilience from a technological perspective. Ensuring directly or indirectly, using services of IT third-party providers, the full range of IT-related capabilities needed to address the security of the network and information systems that a financial services firm makes use of, and supports the continued provision of critical financial services.

The Basel Committee presents several principles that are organized across seven categories that banks must consider for being operationally resilient:

Governance: Make use of the existing governance framework to create, manage, and put into practice an effective operational resilience strategy. Enable banks to respond to disruptive events, adapt to them, and then recover and learn from them to reduce their impact on delivering critical services.

Operational risk management: Utilize respective functions in managing operational risk to continuously look for threats from the inside and outside, and potential flaws in people, processes, and systems. Assess essential operations vulnerabilities as soon as possible and then manage the risks in line with their operational resilience strategy.

Business continuity planning and testing: Establish a business continuity strategy and undertake exercises under various extreme but plausible scenarios. Verify capacity to execute crucial activities despite the disruption.

Mapping interconnections and interdependencies: Once key activities are defined, map the internal and external interconnections and interdependencies required to deliver critical operations in accordance with the bank's operational resilience methodology.

Third-party dependency management: Evaluate and manage the bank's reliance on third parties and intragroup entities to deliver essential operations.

Incident management: Manage situations that could interfere with the delivery of vital activities by establishing and implementing reaction and recovery strategies. Incorporate the knowledge gained from prior incidents into improving incident response and recovery plans.

Resilient information technology (IT), including cybersecurity: Regularly test the resiliency of the bank's critical operations—protect, detect, respond, and recover—incorporating appropriate situational awareness, and conveying relevant, timely information.

Operational resilience has been the subject of intense regulatory scrutiny for years. Still, recent events such as technology-based failures, cyberattacks, COVID-19 outbreaks, and natural disasters prove that significant operational disruptions are increasingly likely. Due to the large amount of clients' personal and banking information stored by financial organizations, they are targeted far more often than other industries. The cost has far-reaching implications, including regulatory fines, rebuilding IT systems, and loss of customer confidence and brand reputation. As FSIs drive toward digital transformation, they have additional complications to consider, compared to other types of companies. For example:

- Critical data is split between on-premises servers, multi-location data centers, cloud platforms, and more
- Global digitization is increasing customers' expectations to include 24/7 self-service, instant responses, and personalized experiences across all service channels and payment platforms
- With the ubiquity of ransomware, maintaining data security is paramount for customer trust
- Budgetary cuts hinder the ability to keep the IT infrastructure up to date, leaving it vulnerable and potentially impacting customer experience

The following sections explore specific FSI regulatory requirements and recommendations for providing business continuity and testing, resilient information technology, and cybersecurity to help meet the varied operational resiliency regulations referenced.

Regulatory Considerations for Resilience

Disaster recovery and business continuity is not new. FSIs and regulators globally increasingly recognize that significant disruption from cyberevents, natural disasters, malware, and more will materialize. Therefore, firms must develop recovery strategies for a range of severe impacts. In this context, regulators are thinking beyond more traditional disaster recovery (DR) practices to other methods to secure and recover critical assets.

While DR and business continuity focus internally on the organization itself and its ability to continue to function, operational resilience looks externally, bringing into scope not only customers, but overall market integrity as well as the entire financial system. Operational resilience focuses on a relatively small number of identified important business services, accepts that there will be disruption, and attempts to ensure they remain within the defined impact tolerances.

Identifying and mapping important business services, setting impact tolerances, defining plausible disruption scenarios, and testing against these makes compliance a non-trivial undertaking. These requirements are continual and include the following:

- Review all critical services, continue to assess their importance, and adjust accordingly
- Continually review impact tolerances to ensure validity and acceptability
- Repeatedly test, refine, and evolve plausible disruptive scenarios to reflect an ever-changing regulatory environment

Today, the effectiveness of DR/BC solutions is predicated on the failure of infrastructure in a single location. But malicious cyberevents are often deliberately designed to exploit vulnerabilities in a platform and can impact infrastructure in multiple locations, including primary and secondary sites. Malicious cyberevents can also corrupt data stores as well as backup solutions.

Thus, the importance of focusing on operational resilience:

- Conventional disaster recovery—individual component, system, platform, or data center level
- Minor incident with little impact—local clustering
- Major incident with potential for significant impact—failover to a geographically separate instance
- Severe disruption—hosts rebuilt from bare metal and data recovered from backup
- New Data Vault—recovery of business independent of the FSI's existing technology environment
- Extreme recovery scenario—all other recovery options are exhausted and must recover from data in the vault

The key components of the regulations are summarized below:

The European Commission

FSIs must use and maintain updated IT systems appropriate to the demands of their critical operations and services. These systems must be reliable, have sufficient capacity to meet the varying demands of the services, and be technologically resilient to deal with stressed market conditions, especially where an exit from a managed service provider or cloud service provider is required.

IT systems must be monitored and be able to detect anomalous activities to minimize the impact of any operational risks. This will require FSIs to implement dedicated and comprehensive IT business continuity and backup and recovery solutions to ensure the resumption and/or restoration of IT systems with minimum downtime and limited disruption. Different systems from the production environment should be used when resuming operations or restoring backup data to internally owned systems. These different systems should not be directly connected with the production. They must be securely protected from any unauthorized access or corruption. Additionally, recovery must be allowed for all transactions at the time of disruption, to allow FSIs to continue operations uninterrupted and with certainty.

Organizations must establish, maintain, and review a comprehensive digital operational resilience testing program. The testing tools and systems must provide for the testing of a wide range of situations, including vulnerability assessments and scans, gap analysis, scenario-based tests—not just discrete systems or components. End-to-end resumption or recovery of critical business services should also be tested.

UK Prudential Regulation Authority

FSIs must set impact tolerances at the point at which any further disruption to the critical business services would risk their ability to provide the services. The tolerance must include a time-based metric to measure the level of disruption, which will trigger the appropriate recovery operations. Organizations also need to consider other metrics. For example, setting impact tolerance in conjunction with the disruption continuing after a certain number of hours, whether they can tolerate a single disruption; and how these disruptions will impact recovery time objectives (RTOs) and recovery point objectives (RPOs) so that they can continue to deliver critical business services within the impact tolerances.

Regular scenario testing must be undertaken to test an FSI's ability to remain within impact tolerances, focusing on recovery and response times to remain within impact tolerances, which will not give rise to different or other types of vulnerabilities. As such, testing should not risk disrupting an entire chain of activities that are critical business services.

Business continuity plans and testing should test a range of scenarios, including contractual agreements for outsourcing arrangements, testing for both parties' ability to implement and test business contingency plans.

US Federal Banking Agencies

Business continuity practices must be periodically reviewed to ensure contingency strategies remain consistent with current operations, risks and threats, tolerance for disruption, and recovery priorities. Confirming that functional testing procedures for assessing the ability of a firm's IT systems to deliver minimum service capacity to critical operations and core business lines are consistent with the firm's business continuity objectives.

Business continuity arrangements must continually be improved as shortcomings are identified, to respond to a wide range of severe but plausible internal and external stress scenarios, including identifying interconnections and interdependencies among critical operations and core business lines affiliates, subsidiaries, and third parties.

Secure and resilient data management systems must be applied to protect information and help a firm identify and detect risks to operational resilience and enhance its ability to withstand disruptions or failures, including elements that depend on third parties. Risk identification, protection, detection, and response and recovery programs must be tested regularly to safeguard critical data's integrity and availability against destructive malware, including ransomware or other similar threats. Recovery from such incidents may include using secure, immutable, off-line storage of critical data. Information systems and controls must be reviewed regularly against common industry standards and best practices. Firms will benefit from using a standardized toolset aligned with common industry standards and best practices to protect, detect, respond, and recover from cybersecurity threats.

Hong Kong Monetary Authority

Preparing for and managing risks to critical operations will require effective and secure data protection, business continuity planning, and testing. This must include third-party organizations supporting the delivery of critical business services to assure and maintain an acceptable level of operational resilience and exit strategies in the event of a failure or disruption at a third party. As such, information technology, including cyber security, must ensure critical information assets' confidentiality, integrity, and availability.

Regular testing exercises should include realistic assumptions and encompass the firm's interconnections and interdependencies. Different types of testing should be undertaken while considering and carefully managing the risks introduced by the testing itself.

Data restoration and recovery must consider careful data extraction and ingestion design, using a secure data repository, and providing a fast means for validation of recovered data. To ensure a secure, cyber-resilient data backup, the following system characteristics must be considered:

- Immutable and controlled data storage by securely encrypting and storing data in isolated repositories with restricted access
- Secured and verifiable systems capability that can leverage AI/ML analytics, allowing the early detection of suspicious activity or cyberthreats
- Air-gapped backup data disconnected and removed from the production data protection systems, with strict access controls and limited, heavily restricted inbound and outbound communications
- Highly durable and available backup data repositories with the capacity to support long histories of backup data, which must be resilient to recover from any ransomware attack
- Heterogeneous and high performance to allow high-speed recovery across multiple operating environments, including third-party services used to provide critical business services

Veritas Response

Availability and Resiliency for the Modern Enterprise

Managing enterprise-wide operational resiliency has historically been a complex problem. For FSIs, it is critical to plan, adapt, and ensure the continuance of business following operational disruptions due to technology-based failures, cyberattacks, pandemic outbreaks, natural disasters, and more. This requires a unified availability and resiliency strategy that spans all business applications. Historically, that strategy has been to deploy multiple independent solutions, leading to high costs and increased exposure to service disruptions.

Veritas provides operationally-resilient strategies focused on application availability, protection, and insights. As a market leader in application availability, Veritas has a long-standing history of delivering innovative solutions for managing IT availability and resiliency. The integration of Veritas data protection, resiliency, high availability, and storage management solutions provides organizations with a continuum of availability that enables a unified enterprise-wide resiliency strategy to satisfy all requirements for conventional disaster recovery, as well as a data vault solution when all other recovery options are exhausted. This solution includes:

- Local and global clustering
- Bare metal and data recovered from backup
- Recovery of critical data from a data vault
- Visibility and reporting of critical data

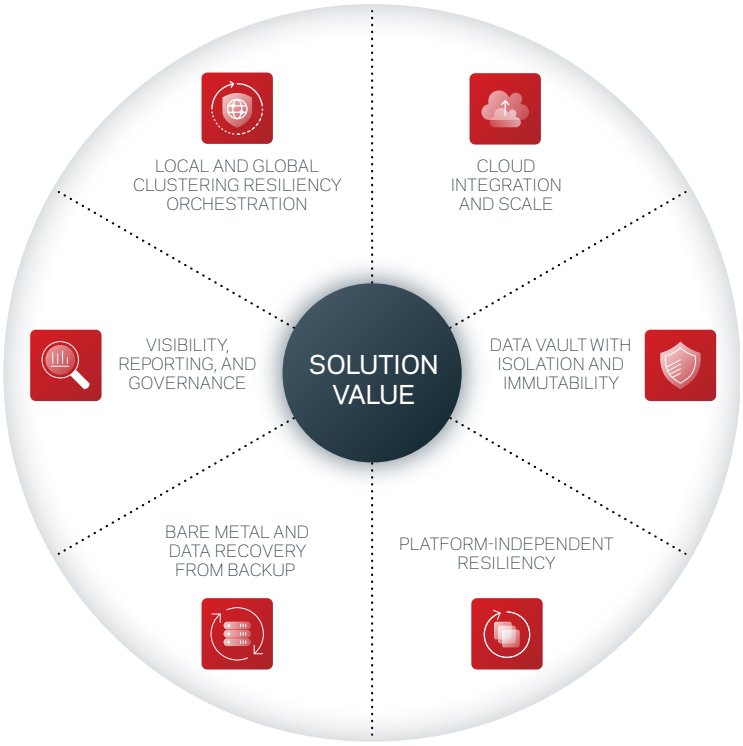
This solution overview will discuss the Veritas strategy for managing operational resiliency for any application, with nearly any uptime requirement. Veritas offers a unique integrated solution that ensures application availability and resiliency for the entire organization, while maximizing your investment in new and existing Veritas technologies.

Solution Value

Veritas reduces complexity and simplifies operations by providing a single platform for visibility and control for availability and resiliency operations, with native integrations that operate as a single solution. This approach allows you to minimize the costs associated with making your applications resilient by enabling you to choose the level of protection required based on your application's business impact. This unified approach has several advantages:

- Flexibility to choose how your applications are protected, based on their business value
- Automated availability management for complex, multi-tiered business applications
- A single solution that provides any RPO and RTO for any application
- Visibility and reporting on availability and resiliency status across the entire organization

Integrating data protection, resiliency, and availability management into a single unified solution provides a continuum of availability for all business applications—unique in the marketplace.



To address the range of operational resiliency requirements needed for the continuity of business, Veritas solutions provide:

Local and Global Clustering and Resiliency Orchestration

High Availability and Data Resiliency Solutions: Software-defined optimization solutions for mission-critical applications that abstracts applications from their underlying hardware and software resources. That abstraction enables enterprise-grade optimizations around business continuity, performance, and infrastructure agility across physical, virtual, and cloud environments. In addition, Veritas provides advanced software-defined storage and availability management for mission-critical always-on applications.

Resiliency Orchestration: Enterprise IT resiliency typically involves multiple systems, processes, and geographic regions. Without automation, managing resiliency can be time-consuming and error-prone. Veritas helps reduce the need for manual processes and provides several intelligent points of automation for the IT resiliency process that help ensure predictability and reliability, maximizing application uptime. You can even include custom applications that require direct interaction with scripts or other application-specific tools as part of an automated resiliency plan. In addition, you can design and build automation plans to manage several resiliency scenarios.

Platform-Independent Resiliency

Modern IT applications can often benefit from leveraging different platforms to achieve optimal performance and utilization. No matter where or how your applications are deployed, Veritas provides several options to make them highly available and resilient. Whether you're looking for on-premises, hybrid cloud, or cloud-only resiliency, Veritas can accommodate nearly any deployment architecture:

- High availability for almost any operating system and platform across local and geographically separated sites
- Support for bi-directional resiliency for physical and virtual systems on-premises or in the cloud
- Multiple supported public cloud platforms, including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform
- Automated recovery of backup images into live systems in public cloud environments

With multiple options to achieve availability and resiliency with a single solution, you can manage availability and resiliency based on the business value and risk associated with application downtime. This flexibility helps you control costs and provides a consistent user experience.

Cloud Integration

The cloud has changed the economics and the approach to IT resiliency. It has effectively eliminated the need to build a second data center dedicated to DR purposes, which allows you to cost-effectively use the cloud as a resiliency and recovery target. But with these pending operational resilience regulations, FSIs must ensure full availability and an exit strategy for any critical applications running in the cloud. And although cloud services offer attractive service level agreements (SLAs), it's important to understand they are not application-aware. As a result, running your applications in the public cloud doesn't eliminate the risk of downtime or data loss.

Veritas provides automated, application-aware availability and resiliency in the cloud to fully manage mission-critical application orchestration. The Veritas solution manages high availability in the cloud with customized agents for mission-critical applications. It also provides storage management capability with enterprise storage features and performance using native cloud storage services. You also have advanced application mobility to move applications and data between cloud zones, regions, and public cloud services.

High, middle, and lower-impact applications that don't require always-on capability can be managed in the cloud with advanced functionality that supports a wide variety of RPO and RTO requirements, including:

- Automated near-real-time replication and recovery for physical and virtual systems into a cloud environment
- Recovery and conversion of NetBackup images into live systems in a cloud environment

Veritas provides a cloud recovery feature—an innovative option for recovering on-premises system backups in the cloud. It lets you restore backup images to the cloud without deploying or managing backup infrastructure in the cloud environment. This option gives you the flexibility of cloud-based infrastructure that can be provisioned on-demand and used only when needed. Cloud recovery of backup images enables a cost-effective hybrid resiliency strategy. It is also an excellent option for cloud migration using existing backup images with minimal resources required.

Bare Metal and Data Recovery from Backup

Data Protection: Veritas provides enterprise-level heterogeneous data protection for nearly any platform and application. It offers cross-platform data protection functionality for various operating systems and applications. Veritas uses a centralized management architecture that can be easily scaled to manage data protection for vast enterprise environments. It has advanced Auto Image Replication (AIR) capability for replicating backup images between sites to maximize resiliency for backup data and backup services. In addition, bare metal restore capabilities are included in the data protection product, allowing complete OS restoration of your Unix, Linux, and Windows servers.

Data Vault Solution

Isolated Recovery Environment (IRE): For enhanced ransomware resiliency, it is important to secure your backup data on immutable storage and maintain an isolated copy of your backup data. This is often referred to as an air-gapped copy. An IRE enables air-gapped backup copies by disabling network connectivity to a secure copy of your critical data, providing administrators a clean set of files on-demand to neutralize the impact of an attack. Our data protection IRE solution:

- Ensures data is immutable and indelible—minimizing threats from ransomware and rogue users
- Detects ransomware infections within the protected data to prevent reinfection when restoring data
- Enables recovery operations at scale, so business services can meet service level objectives
- Enables predictable recovery processes that can be rehearsed to on-premises or cloud infrastructure

Unlike traditional IRE solutions, Veritas offers a unified, scalable solution with immutability and indelibility, and anomaly and malware detection. In addition, Veritas provides an air gap solution that continuously restricts network access to the IRE. Using a pull versus push solution, unlike competitors, Veritas does not need to have any open ports to replicate data to the IRE. As a result, we provide a high-performant solution with zero-trust security, and no extra license cost.

Visibility, Reporting, and Governance of Critical Data

Intelligence and Insights: Holistic real-time visibility into your data and infrastructure status is essential for effectively managing your IT services' availability and operational resilience. Veritas analytics solutions enable you to better understand how resources are consumed on-premise and in the cloud. This allows you to quantify the costs and performance from a hybrid multi-cloud model so that you can optimize your infrastructure and data footprint. It also allows you to ensure that your IT services are protected and resilient by improving data reliability, anomaly detection, automated notifications, and alerts.

Having a clear and complete picture of IT services resource utilization is challenging when using multiple independent tools. Veritas analytics solutions solve this problem by gathering and analyzing more than 30,000 unique data points from storage, compute, backup, and cloud resources as a single pane of glass solution, eliminating the need for multiple independent tools.

Data Compliance and Governance: Digital compliance is the strategy organizations deploy to proactively manage information risk. This strategy requires organizations to effectively identify and catalogue the their most critical information, eliminate information that contains no value, and ensure compliance with all local regulations. Having visibility into the criticality of the data helps when deciding what data needs to be protected for operational resiliency. Of course, all data is not created equal, so your protection needs, such as backup, snapshots, replication, and vaulting, will also vary. Organizations can achieve this strategy through a multi-faceted approach of gaining visibility, providing context, and taking action over information. Successful execution of these steps will remove organizational barriers to information decision-making.

Veritas simplifies this process by illuminating information hazards and providing tools for automated remediation. By delivering a detailed blueprint of your information ecosystem, Veritas arms your organization to fight back against the exponential data curve and reign over risk.

Critical intelligence regarding age, location, and ownership of your organizational information provide the roadmap for effective information decision-making. Understanding the risk profile of your information allows your organization to shift from the store everything mentality to a value-focused perspective. Once organizations have visibility into their information footprint and context from that information, they must act. Ultimately, the choice is between retention, protection, and deletion. By leveraging critical insights into the value of their information, organizations can assign classifications, deploy policies, retrieve what's relevant and initiate clean-up.

Summary

Maximizing application availability and resiliency for complex IT environments can be a significant challenge. With multiple applications and systems with different usage profiles and SLAs, organizations are often burdened with multiple independent products to meet availability and resiliency requirements. Veritas solves this problem by providing a continuum of availability that spans the entire suite of business applications within an organization. In addition, having a single point of control and visibility that can integrate with nearly any application within an organization has several key benefits:

- Single solution for overall availability and resiliency across an entire enterprise
- Full range of availability and resiliency options for all types of applications
- Intelligent automation that eliminates manual processes and maximizes application uptime
- Automated full IT service restores from backups provides operational resiliency using existing backup data
- Minimized costs by choosing an availability and resiliency option based on your application's business value

Veritas is in a unique position when considered in the context of operational resiliency. Most data protection or data security competitors only focus on data. Some vendors address digital compliance at a partial level, but not enough for large financials facing regulations at a global level. Focusing solely on archiving, discovery, and compliance lacks the complete data protection and application resiliency needed. Overall, no other solution matches Veritas in offering data and application resiliency, while addressing digital compliance comprehensively. In a security or non-security event, Veritas can take care of the repair and replace steps with minimal churn to the technology used by customers. Cloud service providers such as Microsoft may come the closest. However, a single cloud provider brings IT concentration risks. Thus, being cloud, storage, compute, network, and communication platform agnostic, Veritas is uniquely positioned to partner with large financial institutions to address and execute against upcoming and ever-evolving operational resiliency regulations.

To learn more about our solutions, visit veritas.com or contact us at veritas.com/form/requestacall/requestacall.

References

- European Commission:
  Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector
- UK Prudential Regulation Authority:
  Supervisory Statement SS1/21 Operational resilience: Impact tolerances for important business services
- US Federal Banking Agencies:
  Sound Practices to Strengthen Operational Resilience
- Hong Kong Monetary Authority:
  Supervisory Policy Manual Operational Resilience

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1805 06/23