WHITE PAPER

Operational Resilience for Financial Services

Rubrik Cloud Data Management

April 2020

TABLE OF CONTENTS

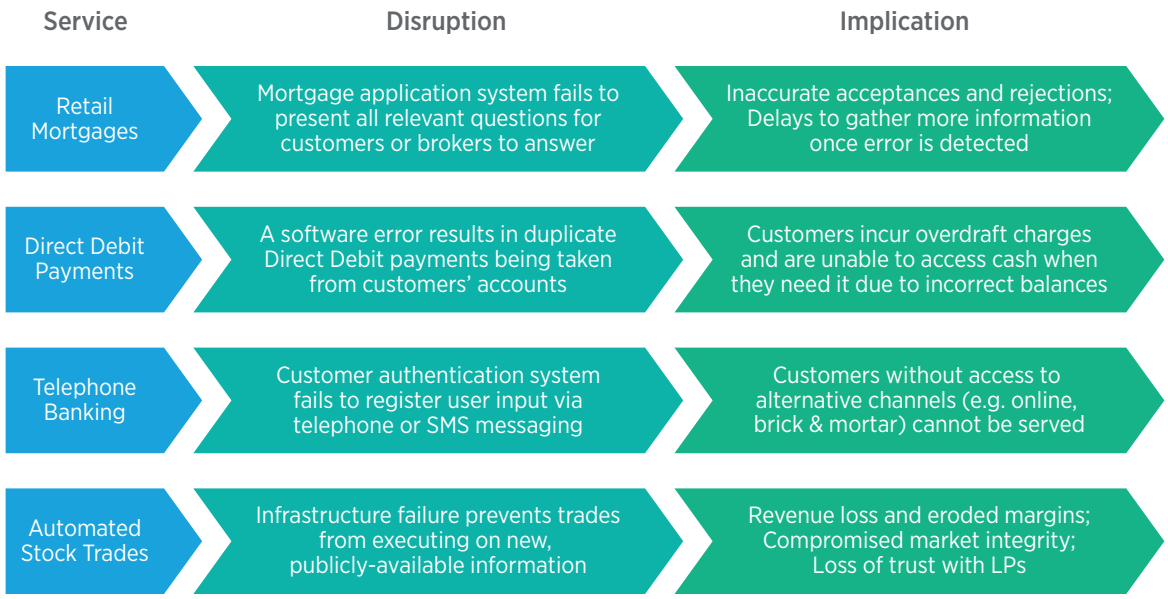
ABSTRACT

Operational resilience is the ability for firms to prevent, adapt, respond to, recover, and learn from operational disruptions. Increasingly, governing bodies and regulators are requiring financial services firms, and by extension, the services that they provide, to be operationally resilient. In order to help the financial sector become more resilient, industry regulators have proposed a stringent set of policies and procedures, but adherence to these policies alone does not ensure that firms can recover swiftly in the event of large, enterprise-scale disruptions. Firms are left to decide for themselves how exactly they intend to achieve *operational resilience*, much of which will be decided by the quality of their investments in IT and data management solutions.

This paper includes information about the latest financial regulations, the various scenarios which threaten the continuity of financial services, and how Rubrik simplifies the delivery of *operational resilience* at scale.

INTRODUCTION

The financial services sector is naturally intertwined with the health and continuity of the global economy. Individual retail and business consumers, insurance providers, mortgage lenders, and even national banks rely on one another to authorize and execute billions of transactions daily. Underpinning each of these transactions is a global network of infrastructure that must remain available in order for financial markets to operate. Without the *operational resilience* of these infrastructures, and by extension the financial services that they support, market participants cannot transact and the integrity of financial markets is put at risk. The figure below illustrates the potential implications of several financial services disruptions.



Sample services and disruptions provided by The Bank of England (DP 01/18; CP 19/32; CP 29/19)

FOUNDATIONAL PROPOSALS FROM THE BANK OF ENGLAND

In July of 2018, the Financial Conduct Authority (FCA) and The Bank of England's Prudential Regulation Authority (PRA) published a first-of-its-kind Discussion Paper to standardize *operational resilience* for the financial sector (see: Building the UK Financial Sector's *operational resilience*). The proposal outlined procedures for financial services firms to identify their most important services, potential risks to the continuity of these services, and the disruption scenarios in which they may or may not be able to recover in a timely manner.

> ***Operational resilience:*** *The Bank of England defines operational resilience as the ability for firms to prevent, adapt, respond to, recover, and learn from operational disruptions.*

Since its release, the Bank of England has received positive feedback from a variety of financial services firms, prompting the Bank to release a December 2019 dossier of Consultation Papers from the FCA, the PRA, and a jointly-issued summary from both.

The paper proposes the following methodology to achieve *operational resilience*:

1. **Identify Important Business Services:** Firms are required to identify which of their services (e.g. retail mortgages, private wealth management, etc), if disrupted, would "cause harm to consumers and market participants, threaten the viability of firms, and cause instability in the financial system".

2. **Set Impact Tolerances:** Once *important business services* have been identified, firms must decide their maximum tolerable levels of disruption (e.g. maximum tolerable duration, number of customers affected, reputational damage, financial loss to consumers or the firm, etc.).

3. **Map Resources:** Firms must identify and document the necessary resources (e.g. people, processes, technology, facilities, and information) required to deliver each *important business service*.

4. **Test Disruption Scenarios:** Firms must test their ability to operate within *impact tolerances* in the event of "severe but plausible" disruption scenarios.

5. **Manage Third-Party Risk:** Firms have full responsibility for meeting their *impact tolerances* and cannot delegate any part of this responsibility to third-parties. Therefore, firms must remain Operationally Resilient regardless of their use of third-party IaaS, PaaS, and SaaS providers.

6. **Develop Communication Plans:** Firms must have procedures in place to immediately communicate disruptions to internal and external stakeholders.

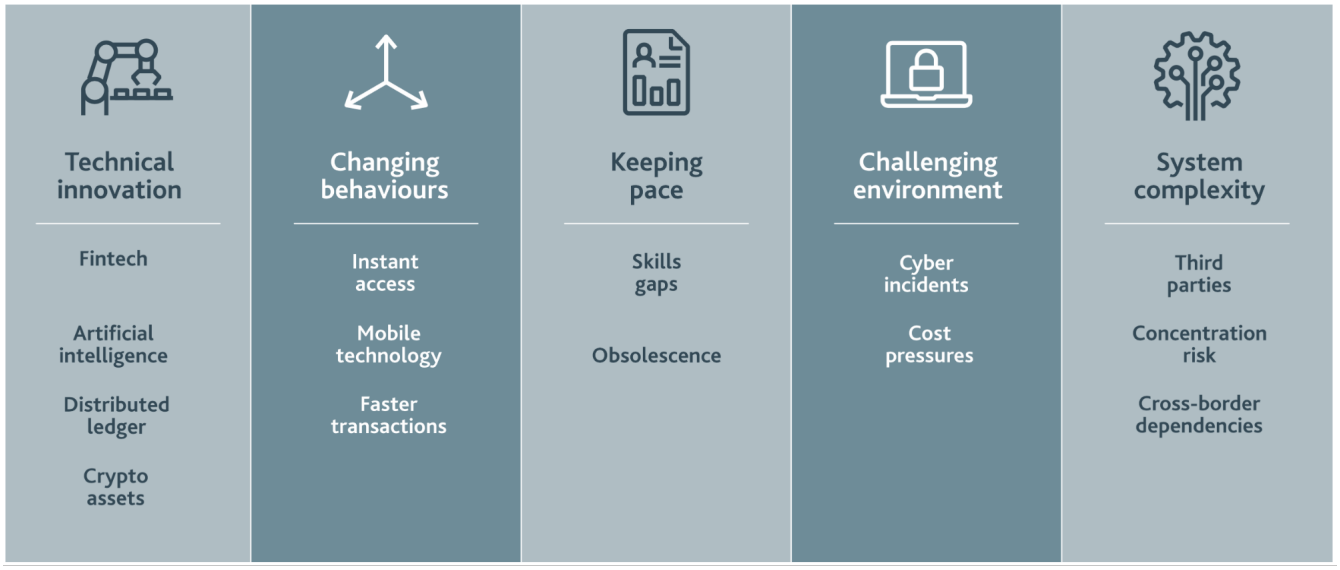
7. **Conduct Self-Assessments:** Firms are expected to generate reports on their *important business services*, their corresponding *impact tolerances*, and the scenarios in which they expect to recover in a compliant or non-compliant manner.

8. **Report to Board of Directors:** Firms are required to report their *important business services*, *impact tolerances*, and *self-assessments* to their Board of Directors in order to maintain third-party oversight.

9. **Invest in Operationally Resilient Solutions:** Lastly, once firms have identified vulnerabilities to their *operational resilience*, they are required to invest in solutions that enhance their ability to recover in a compliant fashion (e.g. within their *impact tolerances*).

Although the policies are prescriptive, financial services firms still face a variety of challenges in building Operationally Resilient infrastructures. The Bank's initial Discussion Paper classifies these challenges into five key categories, outlined in the figure below.

Challenges to Building Operational Resilience



Challenges provided by The Bank of England (DP 01/18)

Cumbersome, legacy infrastructure solutions compound many of these challenges, such as the requirements for instant data accessibility, cost efficiency, and defense against cyber threats. In order to mitigate, financial services firms are increasingly requiring their data management solutions to deliver on initiatives such as cloud adoption, automation, data security, and disaster recovery. In fact, the regulations require firms to make such IT modernization investments if existing solutions cannot reliably guarantee compliance.

While the policies are prescriptive with regard to the need for investment, firms are still responsible for determining the exact tactical details of how they will achieve *operational resilience*. For example, an insurer may be required to set an *impact tolerance* for its auto-renewal program, but it is up to them to decide what resources to invest in and to what extent.

Furthermore, the policies require firms to take a new, service-oriented approach to investing in IT modernization. Where firms may have previously upgraded IT systems based on susceptibility to failure, anticipated financial cost of failure, or cost of upgrading relative to available budget, the policies' service-oriented approach redirects attention to stakeholder welfare and business continuity. By viewing IT systems through the lens of the services that they support, firms can develop better purchasing requirements based on the needs of their customers.

INTRODUCTION TO RUBRIK CLOUD DATA MANAGEMENT

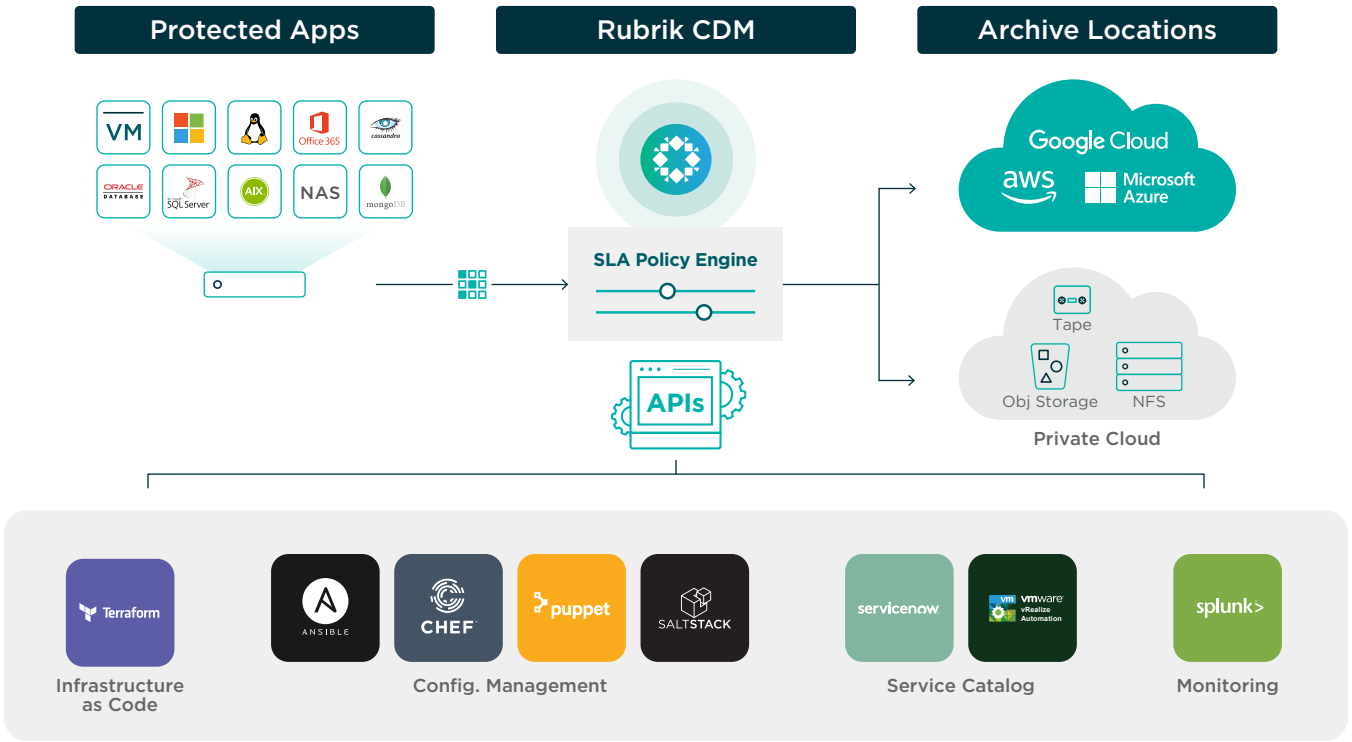
Rubrik simplifies the delivery of *operational resilience* through a single software platform for data management across hybrid, multi-cloud environments. Rubrik has been designed from day one to automate data protection, accelerate the cloud journey, and unify data management across global data silos. In the event of enterprise-scale disasters, breaches, and failures, financial services firms rely on Rubrik to deliver *operational resilience* and business continuity at scale.

Rubrik's product portfolio includes the following:

Rubrik Cloud Data Management (CDM): Rubrik's flagship data management solution was designed to deliver on key initiatives for automation, scalability, and ransomware defense across hybrid and multi-cloud environments:

- **Automation:** Rubrik's single SLA policy engine automates backup, recovery, archival, and disaster recovery for physical, virtual and cloud-native workloads. With our API-first architecture, users can also integrate with any automation tool of choice to reduce management time by up to 90% or more.
- **Scalability:** The CDM platform enables seamless scaling of backup data across on-prem and cloud. Users can scale backups on-prem with Rubrik's linear-scale architecture, or simply leverage the cloud for its grow-as-you-go economics.
- **Ransomware defense:** CDM is built with an immutable filesystem, meaning cyber attackers cannot overwrite backups. In the event of an attack, financial services firms can simply recover in minutes.

Rubrik Polaris - The Data Operations Platform: Polaris captures metadata from your global Rubrik CDM deployments, enabling unified visibility across your data landscape. With Polaris, financial services firms can repurpose their backup data for new, value-added SaaS applications, such global monitoring and management, AI-driven ransomware remediation, and automated data classification.



SAMPLE OPERATIONAL RESILIENCY PLAN WITH RUBRIK

Below is an example of how financial services firms can use Rubrik to simplify the delivery of *operational resilience*.

IDENTIFYING IMPORTANT BUSINESS SERVICES

The Bank of England proposes that an *important business service* should have the following characteristics:

- It should be clearly identifiable as a separate service, as opposed to a collection of services.
- The users of the service should be identifiable so that the impacts of disruption are clear.
- It should include a consideration for all parties affected by the disruption, such as the firm's consumer base, the broader financial system, and the firm itself.

Given the above, a retail bank may reasonably choose its retail mortgage service as its single most important service. The service can be clearly distinguished as a line of business, can be traced to individual customers, and if disrupted, could have massive implications for consumers and the business alike.

SETTING IMPACT TOLERANCES

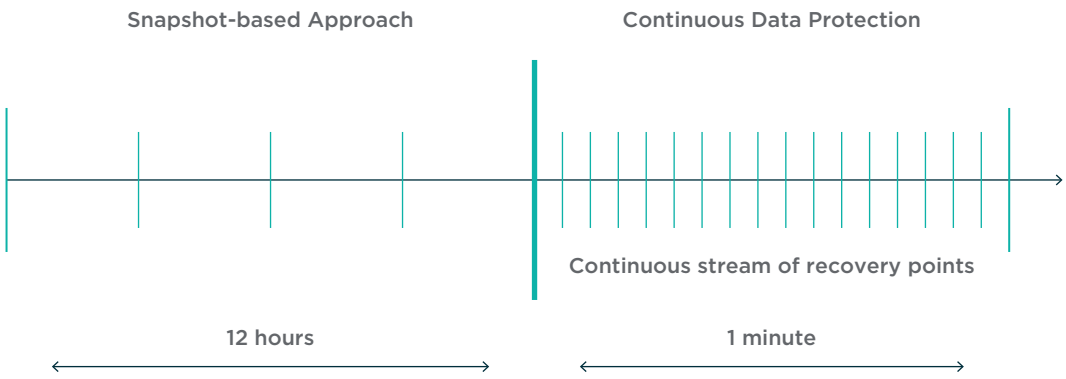
In addition to preventive measures that keep threats out, financial services firms are required to invest in solutions that accelerate recovery and minimize business impact when disruption inevitably does occur. Rubrik fits directly into this defense-in-depth approach as the last line of defense, ensuring that firms can reliably comply with *impact tolerances* when called upon. On setting *impact tolerances*, the FCA has provided the following guidance:

> *... Firms should set their impact tolerances at the first point at which a disruption to an important business service would cause intolerable levels of harm to consumers or market integrity. We consider that firms are best placed to determine the point at which to set their impact tolerance, taking on board the needs of their customers.*

To provide firms with flexibility in prioritizing their services, Rubrik offers a breadth of data protection and recovery options. For business services with stringent *impact tolerances* pertaining to data loss, Rubrik natively-integrates features like Continuous Data Protection, which enable near-zero RPOs. This means that in the event of a disruption, users can restore the application up to seconds in the past, thus minimizing data loss. Together with features like Instant Recovery, firms can also achieve near-zero RTOs, minimizing business downtime, reputational damage, financial loss, and more. Regardless of the metrics used for each *impact tolerance*, Rubrik can easily be configured to simplify compliance for your service level agreements.

NEAR-ZERO RTOS

An application's RTO is simply the time required to restore the application and resume operations. Rubrik's Instant Recovery feature allows enterprises to prioritize their most critical applications by restoring them in seconds – in other words, with near-zero RTOs. If the continuity of a business service is contingent on the availability of a critical database or cluster of VMs, users can leverage Instant Recovery to comply with their *impact tolerances*.



NEAR-ZERO RPO

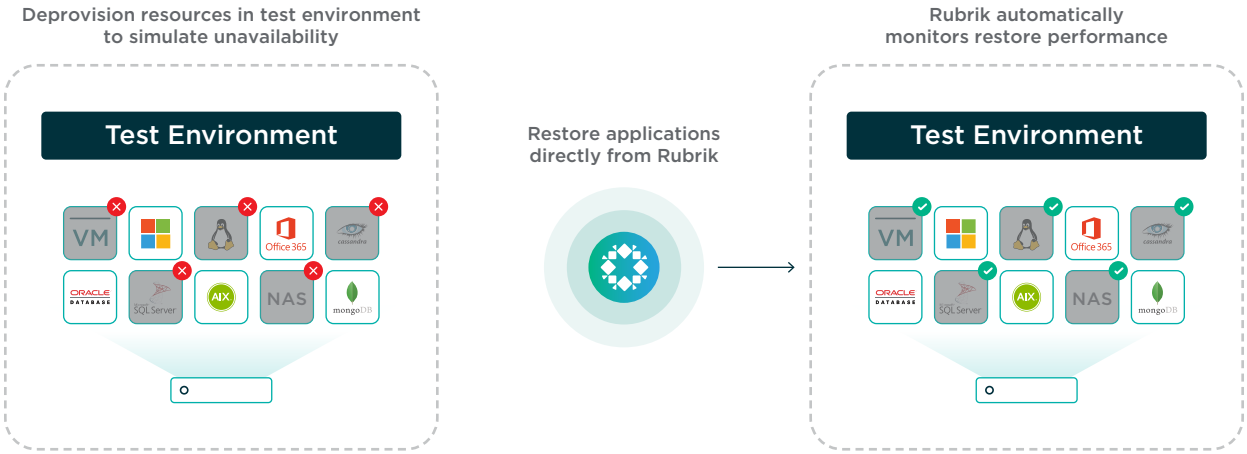
For *impact tolerances* pertaining to data loss, Rubrik's natively-integrated Continuous Data Protection (CDP) enables near-zero RPOs. With CDP, users can recover applications to any point-in-time up to seconds in the past, ensuring seamless recovery in the event of any large-scale breach, failure, or disaster. Customers commonly use CDP to protect their most critical services running on virtual infrastructure.

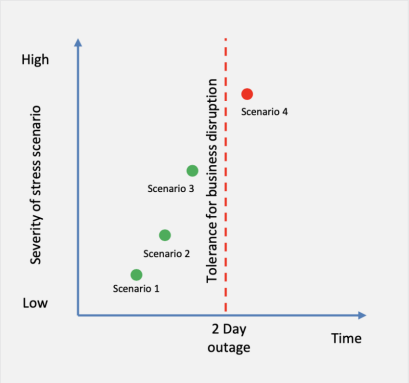
SCENARIO TESTING

Regulators require firms to test their ability to remain within *impact tolerances* in the event of "severe but plausible" disruption scenarios. For regulators, the tests confirm that *impact tolerances* are set, are monitored, and that they can be met. The FCA has provided the following guidance on determining the scenarios that need to be tested:

- Use the *mapping* to identify the most critical resources for your *important business service*.
- Vary the severity of the tests by increasing the number or type of resources left unavailable, or by extending the period for which a particular resource is unavailable.
- Test additional scenarios accounting for failures outside of the firm's control, such as disruption to power, transport or telecommunications infrastructure.

To conduct the tests, users will need to create a test environment and protect it with Rubrik. Once protected, users can harmlessly deprovision workloads knowing that Rubrik can restore them back directly. When recovering the workloads, Rubrik automatically reports metrics on the size and speed of the recovery. These metrics can later be used for generating *self-assessments* and reports.





Sample test results provided by The Bank of England (DP 01/18)

CONDUCTING AND REPORTING SELF-ASSESSMENTS

Rubrik tracks restore speeds and exposes the metrics via APIs, enabling a breadth of reporting methods to Executive Management.

The Bank of England has provided a sample visualization (see: left) that demonstrates the linear relationship between simulation severity and recovery time.

Note that firms are only required to recover within *impact tolerances* for "severe but plausible" disruption scenarios. In the example provided, "Scenario 4" may be considered disproportionately extreme, and therefore can be exempt from the policy.

ENABLING REPORTING AND PROCESS EFFICIENCY

Rubrik is the industry's only data management solution built on an API-first platform, meaning that all capabilities available through Rubrik's UI are also available through the REST API endpoints. In the event of a large-scale failure, users can invoke Rubrik API's to initiate a mass recovery and to propagate alerts through any IT service portal of choice. This not only expedites and automates recovery processes, but also simplifies compliance with *communication plan* requirements.

By integrating Rubrik with monitoring tools such as Splunk or Nagios, financial services firms can stream information on compliance, infrastructure health, and application consumption directly into a single dashboard for centralized consumption in an easy-to-use web interface.

With the service catalog integrations, users can leverage self-service access for data protection, instant recovery, application test/dev, and customized analytics. Users eliminate lengthy wait times at the help desk by accessing Rubrik directly from their service catalogs, further accelerating recovery in the event of a disruption to an *important business service*.

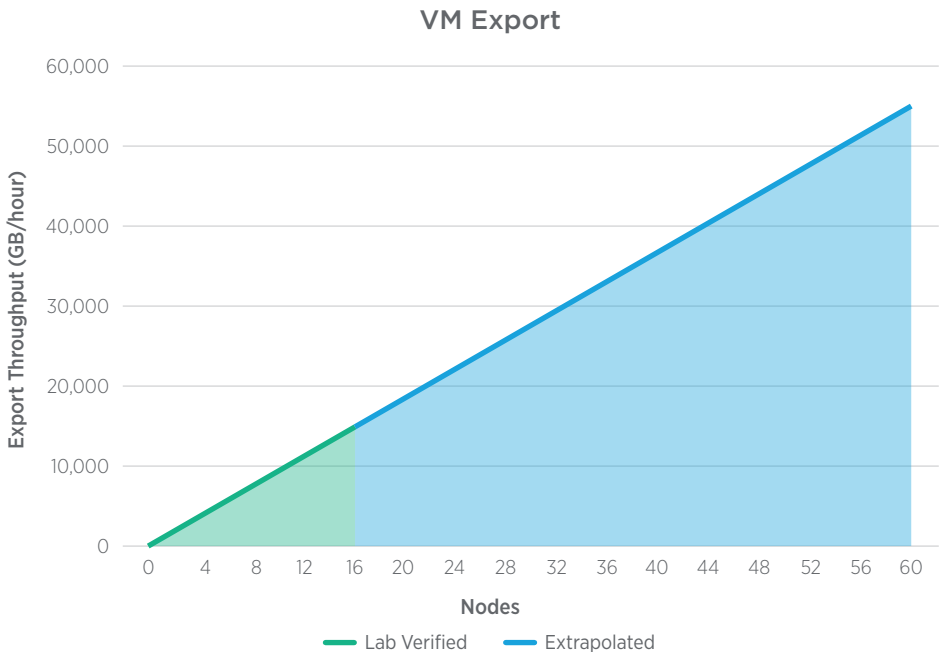
DISRUPTION SCENARIOS AND RECOVERY PERFORMANCE

LARGE-SCALE OUTAGE

In the event of a large-scale outage, firms can use Rubrik to restore their most *important business services* with rapid throughput. For virtualized workloads, Rubrik offers a variety of recovery options, but customers tend to focus on the following for large-scale disaster scenarios:

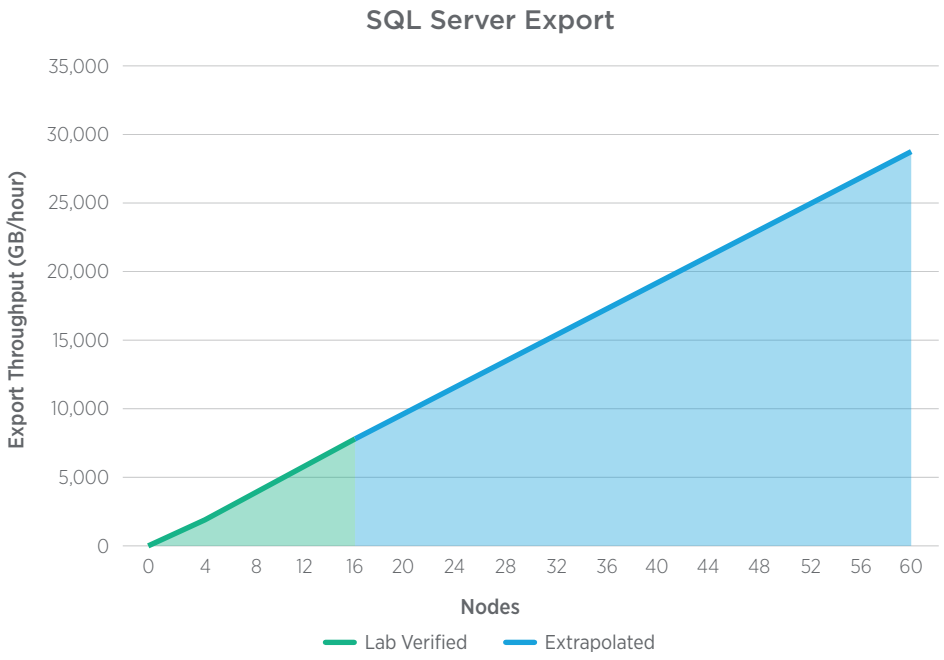
Feature	Used For	How it Works	RTO
Instant Recovery	The most critical VMs that are used to manage and operate the *important business service*. There are typically between 50-100 workloads of this type in the average large enterprise	Rubrik spins up a VM snapshot directly on the CDM platform and uses it as live storage. The platform intelligently leverages the ESXi host for compute resources while keeping the original VM intact.	< 60 seconds
Export	Second tier VMs that are not as critical to the life of the business service.	Export works the same as Instant Recovery, except that the existing production VM is deprecated and replaced with the newly provisioned compute resources on the ESXi host.	< 60 minutes

The graph below illustrates Export performance at scale. A key detail to note is the granular scalability of the platform. Each Rubrik "Brik" is 4 nodes, allowing users to scale linearly just as one would in the public cloud. In the context of DR planning, financial services firms can simply size the VM footprint of their *important business service* and purchase the appropriate number of Rubrik nodes to recover within their *impact tolerances*. Rather than maintaining a DR site complete with infrastructure that may largely remain idle, utilizing the cloud for on-demand recovery and restores delivers overall cost savings while enabling resiliency in operations.



BUSINESS-CRITICAL APPLICATION FAILURE

The continuity of an *important business services* may commonly be hinged on a single large, hyper-critical application. We have commonly seen customers use Rubrik to restore these critical customer-facing workloads running on large databases such as Microsoft SQL Server or Oracle. For both, Rubrik offers the same breadth of recovery options as available for virtual workloads, providing features such as Instant Recovery, Export, and Live Mount. The graph below illustrates Rubrik's Export performance for SQL Server at scale.



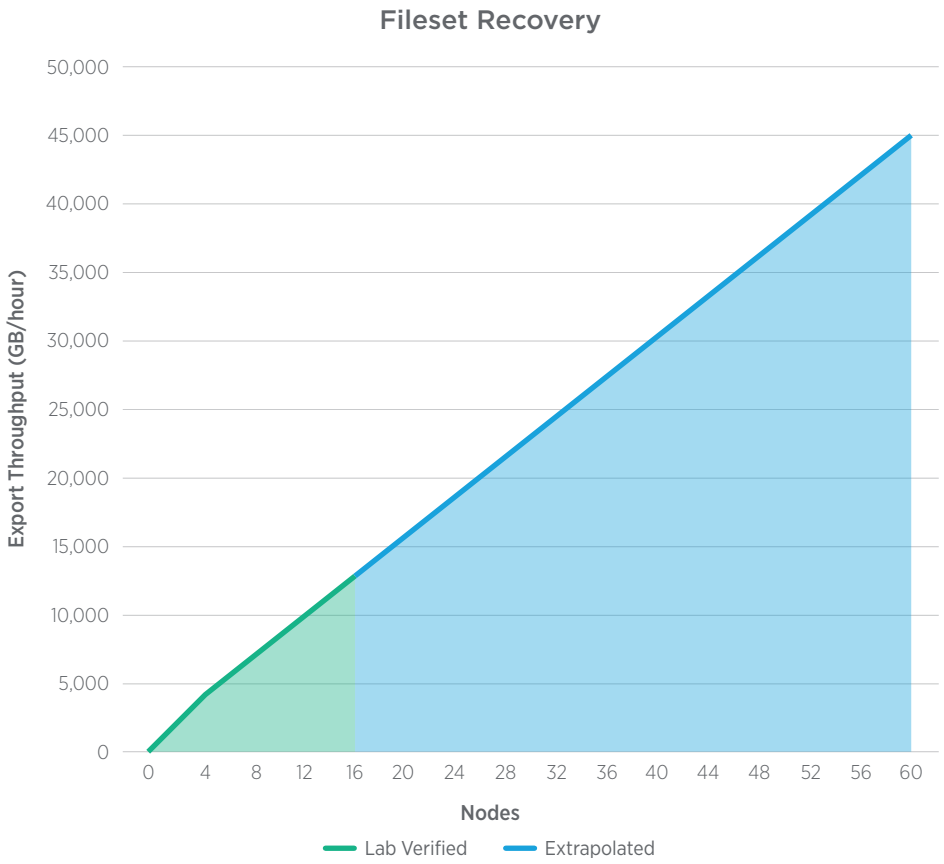
Live Mount in particular is a feature that drives tremendous value for DBAs in the financial services sector. With Live Mount, DBAs can deliver near-zero RTOs by restoring a database directly on Rubrik. During a Live Mount, Rubrik reads all IO operations directly through a flash tier to optimize performance. DBAs commonly use Live Mount to perform the following:

- **Ad hoc queries and restores:** DBAs can quickly perform selective restores of specific rows or tables. By mounting multiple recovery points, DBAs can easily track changes without provisioning extra space.
- **Health checks:** DBAs can quickly spin up database clones to validate backups without impacting production. With Rubrik's APIs, users can automate the entire validation process with a single script.
- **Test/dev workloads:** DBAs can spin up unlimited database clones without a storage penalty.

> **We were able to grant our SQL database administrators some administrative privileges in Rubrik. Now they can find and instantly restore their own databases without having to submit a request to the backup team.**
>
> **Scott Ament**
> IT Operations Lead, Compeer Financial

RANSOMWARE ATTACK

Ransomware is top of mind for every business, but even more so for financial services firms. Financial data is often among the most sensitive, capable of being traced down to a single individual and causing virtually unlimited financial harm. In 2019, the data breach at Capital One brought even more attention to the issue within the financial services sector, reminding businesses of the importance of securing data across on-prem and cloud. We have seen that on-prem ransomware commonly attacks NAS shares and filesets so that the attack can spread to multiple users and high-touch files very quickly. Rubrik has a deep history of protecting and restoring filesets at up to multiple petabytes in scale.



In addition to robust fileset recovery performance, Rubrik has several capabilities that mitigate ransomware attacks more broadly. Users can leverage CDM's native filesystem immutability to reliably restore backups from any ransomware attack, and also Polaris Radar for even faster, ML-driven remediation.

Feature	How it Works
Filesystem Immutability	Rubrik CDM's filesystem has been designed from the ground up to defend against ransomware with native immutability, meaning that attackers will never be able to overwrite your backups. In the event of a ransomware attack, financial services firms can rely on their backups to be there when they need them most. Since Rubrik also encrypts all backup data in-transit and at rest, there is an added layer of security that prevents attackers from viewing your most sensitive business information.
ML-driven Ransomware Remediation	Polaris Radar helps you increase your resiliency against ransomware by making it faster and easier to recover from an attack. Radar helps you recover faster by providing a simple, intuitive user interface that tracks how your data changed over time. It replaces manual recoveries with just a few clicks for minimal business disruption. It also increases intelligence by using machine learning to actively monitor and generate alerts for suspicious activity.

CONCLUSION

As financial services firms face increasing regulations, they are tasked with investing in solutions that not only simplify compliance, but also drive competitive advantage. The availability of *important business services*, as outlined by The Bank of England, is critical for maintaining business reputation, improving customer retention, and building the foundation for new and more innovative technological services for customers. In an increasingly hostile environment with cyber attacks, insider threats, and unplanned outages, solutions like Rubrik are more valuable today than ever. Rubrik delivers a radically new approach to data management, enabling financial services firms to simplify their requirements for enterprise-scale data protection and disaster recovery.

To learn more about Rubrik Cloud Data Management, visit our website at rubrik.com.

To see it in action, speak to one of our sales representatives at rubrik.com/contact-sales.

ADDITIONAL RESOURCES

- **Webpage:** Rubrik for Financial Services
- **Case Study:** Grove Bank & Trust
- **Case Study:** Compeer Financial
- **Data Sheet:** Rubrik and ServiceNow Integration
- **Data Sheet:** Cloud Data Management for Digital Enterprises
- **Whitepaper:** The Definitive Guide to Rubrik Cloud Data Management

rubrik

Global HQ
1001 Page Mill Rd., Building 2
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

20200521_v1