White Paper

Everpure

Strengthening Operational Resilience in Financial Services

Solutions for addressing the new risk regulations

Everpure

Contents

Introduction 3

Global perspectives on operational resilience for financial services 4

- The EU and UK 5
- The US perspective 5
- Asia-Pacific approaches 6

Key takeaways from global approaches to operational resilience 6

- Breaking it down further 7

Techniques for achieving operational resilience 8

- The tiers of a resilience architecture 9

Operational resilience, cyber resilience, and business continuity 9

How Everpure solutions enable operational resilience 10

- FlashBlade and FlashArray 10
- SafeMode 10
- Rapid Restore 10
- Other features and capabilities: 11

Conclusion: Maximizing operational resilience in financial services 12

Additional resources 12

- Next steps 12
- Supporting information 12

Introduction

For financial services firms, risk management is a responsibility that is both constantly expanding and relentlessly evolving. Ever since the financial shock of 2007–2008, global finance ministers and regulators have continually raised the standards for risk management and have included more and more areas in their definitions of covered activities. At the same time, the addition of new technologies and market developments create additional challenges that must be addressed to ensure the operational resilience of an enterprise.

Regulators and the market in general have come to recognize that an increasingly complex, interconnected, and expansive financial services ecosystem requires that risk management expand dramatically beyond purely financial measures to include the whole of the operation and the ecosystem in which it exists. Increasingly, risk management of the 21st century encompasses all aspects of an operation with a particular focus on the data and technology that underpin modern business. Going forward, operational resilience is a frontier that an enterprise must manage and maintain with discipline and diligence, and not only because it is required by regulators. There are other benefits to be gained through operational resilience, from demonstrating to customers and other stakeholders that your business (and their investment) is secure, differentiating from competitors, and ensuring enterprise stability from losses, failures, or employment instability. Operational resilience is an essential ingredient for the modern enterprise.

Operational resilience refers to the ability of firms, financial market infrastructures (FMIs), and the sector as a whole to maintain or recover its operations and services in the face of disruptions, disasters, or other operational risks. Broadly, it encompasses the strategies, processes, and systems that financial institutions put in place to ensure that they can continue to provide critical services to their customers, no matter what. Operational resilience has become increasingly important for financial services companies as they face ever increasing risks, including cyberattacks, ransomware, natural disasters, and pandemics.

Looking at this complicated issue from the regulators point of view is a helpful lens for understanding operational resilience in financial services. Starting with the current state of regulation and digging in to see the similarities and differences between geographic regions and where the regulators are focusing their attention, we can then examine the challenges and approaches to managing this difficult subject. In the end, a picture of where the issue of operational resilience is headed will come into focus.

> “90% of resilience professionals expect the threats to their organization to increase over the next three years.”
>
> The Conference Board, August 2023[1]

Global perspectives on operational resilience for financial services

Operational resilience as a risk management function and responsibility is a relatively recent phenomenon. While the related field of business continuity planning began in the 1970s (see sidebar), operational resilience came to the fore beginning in 2017. Regulators from Europe, Singapore, Hong Kong, the US, and elsewhere, reacting to an epidemic of cybersecurity events and the rise of ransomware, recognized that risk management for the enterprise needed to move beyond financial measurements to encompass all aspects of operations, particularly because information and communications technologies (ICT) are now the backbone of the modern enterprise. Logically, cyber resilience has been central to these efforts; a preeminent concern in a constellation of critical issues as regulators and businesses recognize the interconnections and concentrations that emerged as the concept of "too big to fail" from the global financial crisis. If anything, an increase in concentration and further advancement of digital operations have only raised the stakes.

Since 2017, operational resilience has continued to evolve in a patchwork fashion as each jurisdiction places their own distinct stamp on regulation. This uneven approach and adoption is reflected in the ways that private enterprise has approached the challenge and is a good indicator for how things are likely to develop going forward.

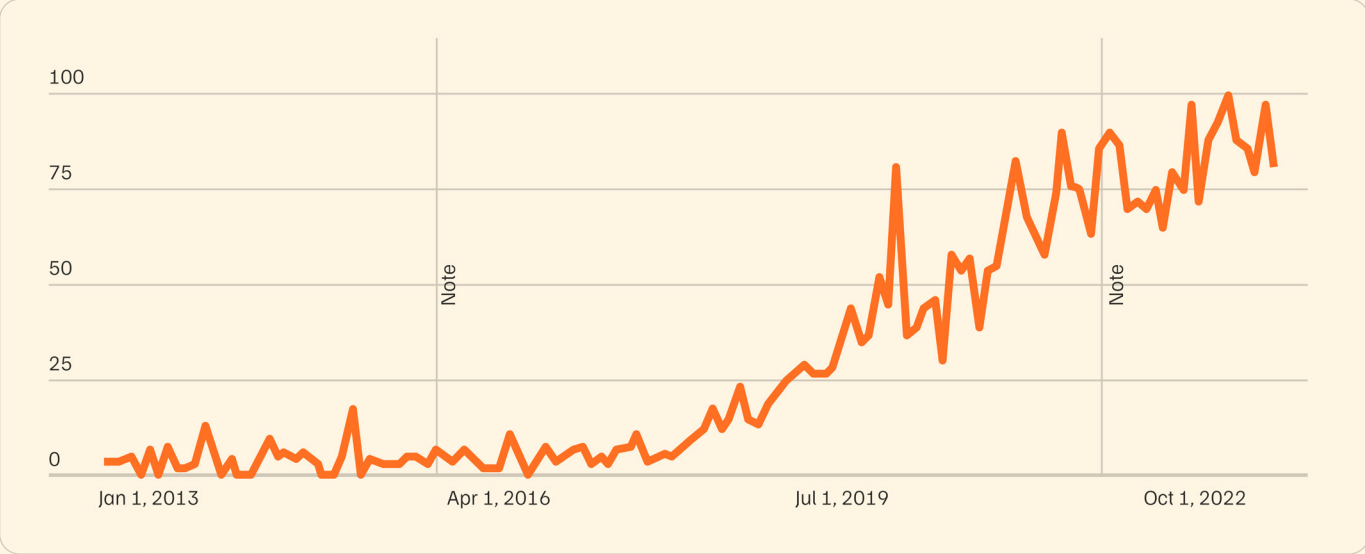

FIGURE 1 Where there's smoke there's fire: internet searches for "operational resilience" increased dramatically beginning in 2018 (Source: Google Trends)

In brief, while the issue of operational resilience began to emerge as an issue for all global regulators beginning in the mid-2010s, the approach to dealing with the issue is very different in specific geographic regions and the pace of implementation varies a great deal as well. Specifically, the EU and UK lead both in terms of implementation timelines and the level of prescriptiveness in regulations while the US is following a more collaborative but disjointed approach and efforts in APAC are strong in some regimes but less so in others.

The EU and UK

The EU has adopted the most far-reaching and prescriptive regulations for operational resilience. A first draft of the Digital Operational Resilience Act (DORA) was published in September 2020 and the regulations are now slated to take effect from January 17, 2025. DORA was developed from the 12 principles for operational resilience (the POR), which were published in 2021 and built on the Basel Committee on Banking Supervision's Principles for the sound management of operational risk (the PSMOR), originally issued in 2011 and revised in 2014 and 2021.[2] DORA is a comprehensive framework that unifies processes and standards across the financial sector. It ensures that all participants in the financial system, including FinTechs and third-party service providers, are subject to a common set of standards to mitigate ICT risks for their operations.

Key aspects of DORA include establishment and ongoing maintenance of security policies, risk management principles and frameworks, robust and active user awareness training, and regular audit and testing of security processes and systems. While there is no stipulation of fines and penalties written into the DORA regulation, individual EU nations may impose penalties and criminal sanctions, which can include fines of up to 2% of a firm's total annual global turnover.

For more information on DORA, read our blog: DORA 2025: How's Your Operational Resilience Holding Up?

The UK has also been active when it comes to developing and adopting guidelines for operational resilience and, in fact, levied a nearly £50 million fine in December 2022 for an operational resilience incident at a UK bank.[3] Responding to increasing awareness of cyber vulnerabilities, the Financial Conduct Authority (FCA) along with the Bank of England (BoE) and the Prudential Regulation Authority (PRA), promulgated their operational resilience policy in March 2021. The policy emphasizes the need for financial firms to improve their resilience against operational disruptions and requires them to establish plans to respond to severe but plausible risks. The rules went into effect in April 2022 and firms have a three year transition period until 2025 to be in continual compliance with their plan guidelines.

The substance of the regulations requires that firms define and defend critical business services and then determine the levels of disruption that can be endured for the enterprise to continue to deliver vital functions. From there, regulations require that firms conduct mapping and scenario testing, with a strong emphasis on communications strategy and internal abilities for self-assessment of performance, particularly when it comes to recognizing weaknesses or vulnerabilities.

In short, the principals for the FCA, BoE, and PRA are to prevent, adapt, respond to, recover, and learn from operational disruptions.

The US perspective

In contrast to the EU and UK, the development of operational resilience in the US has been based on bottom-up advisory and interagency cooperation rather than top-down regulation. Central to these efforts is the Cybersecurity and Infrastructure Security Agency (CISA). It was created in 2018 and is a part of the Department of Homeland Security. CISA's responsibilities include risk assessment, vulnerability reduction, threat detection, incident response, and recovery efforts with other federal agencies, state and local government, and the private sector. CISA's focus is on voluntary collaboration and providing resources, such as risk management tools, threat assessment, and training, to harden US infrastructure and help entities improve their cybersecurity.

Some responsibility in the US also lies with the Federal Financial Institutions Examination Council (FFIEC) but it has a much broader, less specific mandate. FFIEC is an interagency body composed of the heads of the five federal banking agencies: the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau. In general, their role is coordination and advisory, not regulation per se. The Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) also review firms' operational resilience practices as well as their ability to prevent interruptions to critical services and to protect investors' data, records, and assets.

The White House released a National Cybersecurity Strategy in the Spring of 2023. It also had a broad mandate that extended beyond financial markets to include areas such as energy infrastructure and healthcare systems and it, like most other efforts in the US, also relied more on cooperation than regulation.

Asia-Pacific approaches

In APAC, Singapore and Hong Kong have been the most active and direct when it comes to establishing operational resilience practices while other financial centers, including Australia, Japan, and Malaysia, are addressing cybersecurity requirements and more but with a more limited or conservative approach.

The Monetary Authority of Singapore (MAS) first introduced business continuity management (BCM) guidelines beginning in 2003 and has continued to expand and refine their approach over the years. Revised guidelines that are much closer to the stricter, more comprehensive parameters of operational resilience were finalized in June 2022 and financial institutions are now "on the clock" to come into compliance. A plan that meets the regulatory requirements as well as an audit regime were required by June 2023 and a first audit must be completed by June 2024.

To comply, a financial institution must adopt a holistic end-to-end view of the critical business services' dependencies that considers the complete set of processes involved. While business continuity concepts like service recovery time objectives (SRTOs) are mandated, the regulations also recognize the complexity created through critical third-party relationships and the fact that some aspects of services must be prioritized over others during a protracted and staged recovery process.

In Hong Kong, the Hong Kong Monetary Authority (HKMA) issued a circular on operational resilience, OR-2 Supervisory Policy Manual, in May 2022 that aligned with Bank for International Settlements (BIS) standards that were promulgated in 2021. The first phase of the new regulation, which ended in May 2023, included the requirement that an operational resilience framework be completed along with a timeline for full compliance. The second phase stretches until May 2026, at which time financial institutions are fully functional with their operational resilience plans.

OR-2 requires institutions "to conduct scenario testing for severe but plausible events, establish more comprehensive risk management policies and frameworks specific to the critical business operations identified, and to implement robust incident management programs—the requirements for which go over and above existing business continuity planning and operational risk management frameworks. Financial institutions are required to showcase, through testing plans and reports, that they have effectively defined and implemented scenarios that adequately assess critical operations."[4]

Key takeaways from global approaches to operational resilience

Given the complexity and divergence of approaches from global regulators regarding operational resilience, a financial services company might look to take the easy way out and only look at those regulations that apply directly to their particular region or geography. This would be a short-sighted approach, however, because regulations can reach outside of one territory to affect another. DORA, for instance, applies to all financial services firms doing business in the EU, and that includes all of the companies that supply them with technology and communication services. This list covers payment processors, digital money vendors, accounting information service providers, management companies, insurers, data services providers (including cloud and data center services) and hardware services. The sweep of firms affected is both broad and deep in ways that have never been seen before. In short order, there will be no escaping the scope of operational resilience regulations and mandates.

With that in mind, it is helpful to look at the common threads that define the global approaches to operational resilience. Specifically, there is an emphasis on a shared approach that includes setting cybersecurity standards with required compliance, mandated testing, an emphasis on incident reporting, and a broad mandate for resilience across critical industries, not just financial services.

> "Operational disruptions can cause wide-reaching harm to consumers and pose a risk to market integrity, threaten the viability of firms, and cause instability in the financial system."
>
> FCA—UK REGULATOR[5]

Breaking it down further

Cybersecurity focus: Not all operational resilience issues originate within the ICT or cyber realm but ultimately they all impact the technological backbone of the modern enterprise. For this reason, cybersecurity is central to these efforts, with a strong emphasis on awareness and preparedness for ransomware episodes. The emergence of ransomware-as-a-service as an industry unto itself as well as continued growth in state-sponsored ransomware illustrate how this threat continues to evolve and grow. Cyber events also tend to be more far-reaching and pervasive than traditional operational outages. They can take significantly longer to remediate and recover from, and are generally much more high-profile and costly.

Focus on critical infrastructure and services: An old school approach to business continuity followed a "high wall, deep moat" model that failed to differentiate between core and incidental operational elements. That approach is no longer effective (if it ever was!), making it necessary to have an approach that emphasizes maintaining as much business function as possible in the face of a disruption. The plan must be both comprehensive and flexible. For example, it is now critical to make distinctions between critical and less critical elements of an enterprise so that emergency plans ensure that the enterprise can "keep the lights on," even if it is at a diminished capacity.

Risk management—scope: As previously discussed, risk management was once a purely financial measurement, but those days are now long gone. The scope of risk management has expanded dramatically with the inclusion of operational resilience as a factor, requiring new and innovative approaches at the enterprise level. Adding resilience factors to financial risk measures fundamentally changes the orientation of analysis and dramatically increases the amount of effort involved.

Risk management—cost: The cost of risk management used to be measured purely in terms of market exposure like Value at Risk (VaR) or Expected Tail Loss (ETL). In that type of regime, the best risk management tools are those that cost the least. In the new world of regulations for operational resilience, risk management becomes many times more complex and multi-faceted, rendering old risk measures obsolete. Going forward, the complexity of compliance means that cost must be measured with an eye toward cost per performance, not just simple out-of-the-box costs. Tools will need to do so much more that simply looking for the cheapest solution that delivers the bare minimum will no longer suffice.

Guidelines and standards: Slowly but surely, guidelines and standards that define operational resilience are emerging. While they have yet to be unified and optimized, in time we can expect that these standards will be expanded and codified. Additionally, firms may increasingly be impacted by regulations outside of their home territory. As the most developed, prescriptive, and likely most impactful regulatory framework, DORA is a good standard to adhere to for most financial services entities and technology providers.

Observability: Out of sight, out of mind is never a good approach to risk management. But traditional monitoring solutions, amassed over the years and across silos, lead to blind spots, performance bottlenecks, and increased Mean Time to Repair (MTTR), and they fail to meet regulators' stringent requirements. As part of an overall resilience plan, financial institutions must adopt a proactive observability approach that enables them to continually monitor data pipelines and utilize automated workflows to detect anomalies, trigger alerts, and enhance mitigation. An ounce of prevention is always better than a pound of cure.

Incident reporting: In recognition of the lightning fast evolution of cyber threats and the relative immaturity of operational resilience regimes, regulators place a heavy emphasis on prompt and thorough incident reporting, both to regulators and to the broader community as well. A traditional reflex to shut down and clam up during and after an event needs to be broken. Going forward, cooperation and transparency in matters of operational resilience will be standard operating procedure.

Third-party risk management: Traditional business continuity tended to treat an enterprise as an island but modern business practices have rendered that concept hopelessly out of date. Newer approaches to operational resilience embrace the reality that planning must extend outward from the enterprise to include third-parties that are both sources of risk and vital elements in the functioning of a financial ecosystem.

Complexity: If it isn't already apparent, the expansion of risk management in financial services to include operational resilience dramatically increases the complexity of the task. Doing so requires new skills and resources, involves more parts of the business, and is much more intertwined due to interdependencies, including those that involve third-parties. In addition, the emergence of digital asset categories like cryptocurrencies and decentralized finance (DeFi) and disruptions from climate change or ESG mandates further complicate the picture.

In sum, operational resilience is a relatively new discipline, but it is quickly developing into one of the most important areas of attention for financial services companies. While we are still in the early days of defining operational resilience as a risk management discipline it's important to recognize that all efforts need to be dynamic and not treated as a one-off event. An operational resilience plan is never "done": it must be tested and maintained in an active and ongoing manner. And as the rules and requirements become increasingly codified, and continue to evolve along with business and technology, the result is clear: in the future, a thorough and powerful approach and practice related to operational resilience will benefit all financial services institutions.

> "There are enormous benefits to be gleaned from improved operational resilience—well beyond box-ticking compliance."
>
> **GUY WARREN, CEO, ITRS[6]**

Techniques for achieving operational resilience

When compared to traditional approaches to cybersecurity or business continuity, operational resilience is far broader and more complicated. Operational resilience acknowledges that there is a good chance that an event will occur and shifts from a focus that is purely defensive and preventive to one that also incorporates an operational plan for what to do when an event happens. Organizations should look to apply both internal and external preparations, including a robust employee education program, communication protocols and a threat management team, both to help prevent incidents and to ensure processes are in place if, or when, an incident happens.

As we've seen, the full landscape of challenges and areas of concern for operational resilience is incredibly broad but one fact is universal: data is always at the heart of the issue. It is data that drives the engine of modern enterprise and it is data that ransomware thieves and other purveyors of cybercrime are in pursuit of in their illegal schemes. Protect your data and you have gone a long way to protecting your business.

A key piece of that data protection comes from an effective tiered resilience architecture including multi-layered recovery utilizing security snapshots in order to achieve the lowest possible recovery times based on the needs and recovery time objectives (RTOs) of the organization. While the ability to recover data is essential, recovery that takes minutes, hours, days or more, may not meet the requirements of the business, your customers, or the regulators. In fact, regulators and financial institutions may designate certain workloads as "Tier 1," and thus require that they can recover with minimal downtime and very little data loss. In the event of a negative event, whether a natural disaster, a cyberattack or even an administrative accident, speed and near-instant recovery are crucial.

While data snapshots are a critical part of the plan, it's important to note that not all data snapshots are created equal. While "immutable" snapshots cannot be modified, with the right privileges, they can be deleted. A truly resilient architecture requires snapshots that cannot be modified or deleted, whether by accident or by bad actor (inside or outside the organization), thereby providing a guaranteed point of recovery. In order to achieve "super immutability," those snapshots must be out-of-band and multi-factor authenticated.

The tiers of a resilience architecture

A tiered resilience architecture is implemented in several tiers or layers of defense, which each serve unique and important purposes. Together they help to build speed and durability into a recovery strategy.

Tier 0

This tier includes (but is not limited to) mission-critical infrastructure such as Active Directory, DNS, and time services. Without these services, little or nothing else in the environment will function.

Tier 1

In this resilience layer, primary data and applications that are mission critical to your business operations, including core databases and application services, along with their defined dependencies, will be hosted. When an incident occurs, an organization should begin recovery at the closest point to the incident, so these will be the primary focus of recovery. If they are unavailable, your organization cannot deliver business services to customers. Tier 1 should house three to seven days of truly immutable snapshots.

Tier 2

The second tier acts as an incident response tier, which organizations can leverage for forensics, incident response, and broader recoverability. This layer acts as a replica archive for storing snapshots offloaded from Tier 1. The archive should be able to store snapshots for the medium to longer term, at least three to twelve months, or longer, if possible, enabling incident response teams to immediately (and seamlessly) obtain a longer-term view into any given incident.

Note: While Tier 2 is meant for storing data for the longer term or meeting data compliance needs, in the event of a major disruption, this layer can also run workloads with slightly reduced performance to keep the business running.

Tier 3

Generally, this third tier acts as the backup tier, providing long-term retention for compliance or historical data, or to restore data for less critical applications that do not require snapshot protection. Organizations can also leverage this tier for backup in the event of an extreme scenario.

Tier 4

Tier 4 provides an optional (but highly recommended) layer of defense made up of a one-way data bunker in case of large-scale disasters. In this layer, organizations can replicate their data to live on a completely separate site. Data bunkers are designed to be highly secure in order to provide an extra layer of durability and they can provide crucial storage for the years of data required by regulators. And if an incident occurs, this tier also enables organizations to dynamically spin up compute on demand to be up and running quickly without needing to move data over long distances.

Operational resilience, cyber resilience, and business continuity

Business continuity and **operational resilience** are two critical but distinctly unique approaches to risk management. While both are tasked with addressing disruptions to a business' normal operation, they have fundamentally contrasting starting points and focus on different aspects of an organization's response to disruptions.

While business continuity (BC) and operational resilience (OR) are different, they are complementary and interconnected. BC is a component of OR, with the latter incorporating more aspects such as overall risk management, **cyber resilience**, third-party management, and crisis management. Both are critical for an organization aiming to maintain service delivery in the face of adverse conditions.

Business continuity (BC) is the better known of the two and focuses primarily on the recovery and restoration of critical business functions after a disruption. A BC plan is reactive in nature, kicking into gear when an incident occurs, and its primary goal is to minimize downtime and expedite the return to normal operations. Typically, BC utilizes a cost/benefit approach to determine the scope and scale of activities.

Operational resilience (OR), on the other hand, is a broader, more proactive concept that not only includes the ability to recover from disruptions but also the ability to avoid or prevent them in the first place whenever possible. Unlike the cost/benefit approach of BC, OR starts from a "black swan" mindset that assumes that the worst is likely to happen. While OR involves the capacity to withstand and rapidly adapt to disruptions, preserving the continuity of the delivery of essential services it goes beyond recovery to include identifying potential vulnerabilities, mitigating risks, and adapting to changes in the operational environment.

From the perspective of this conversation, cyber resilience is the single most important area of concern. Cyber resilience refers to an entity's ability to continuously deliver services in the event of cyberattacks. Unlike cybersecurity, which is designed to protect systems, networks and data from cybercrimes, cyber resilience is designed to ensure that systems and networks are not completely derailed in the event that security is compromised. In the face of increased attacks and growing sophistication of those attacks, cyber resilience is a logical response to the fact that it's now a question of when, not if, a successful cyberattack will occur.

How Everpure solutions enable operational resilience

Everpure™ is ideally suited to supporting the operational resilience data needs of financial services firms. Speed and flexibility is maximized because of an all-flash configuration, recovery in the event of a disruption is optimized, and maximum data security is built in. Everpure supports operational resilience by design.

FlashBlade and FlashArray

High-performance, all-flash data solutions from Everpure are ideally suited to a world that demands more in the way of operational resilience. Enhanced speed, simplicity, and throughput make the enterprise more nimble by design and more capable of meeting the stringent data protection and data-availability service level agreements (SLAs) that are critical to efficient business operations. By providing a highly consistent storage portfolio based on a common architecture (with consistent Purity software, custom flash, and management tools shared across it) usage can be optimized to meet workload requirements and benefit from Evergreen® subscriptions that allow customers to keep up with new threats and challenges nondisruptively.

SafeMode

Everpure also provides robust, built-in data protection capabilities with SafeMode™, which provides always-on snapshots of your data. Built on the "four eyes principle," where only two, independent and pre-defined persons can approve any changes, SafeMode protects data and metadata by creating secure, immutable snapshot copies that can't be deleted, modified, or encrypted, even with administrator credentials. It is efficient, fully functional, flexible, and automatable, making it an indispensable tool for building operational resilience.

Rapid Restore

Operational resilience requires getting back to business as quickly as possible. Rapid Restore, built into FlashBlade®, provides petabyte-scale recovery capabilities to meet the most demanding requirements. Importantly, it dramatically increases the speed of data restoration without the need to change your backup software. Legacy systems are notoriously slow and ill equipped for restore and recovery operations. At the same time, the all-flash architecture of FlashArray™ provides fast backup and restore to overcome the limitations of legacy data protection architectures.

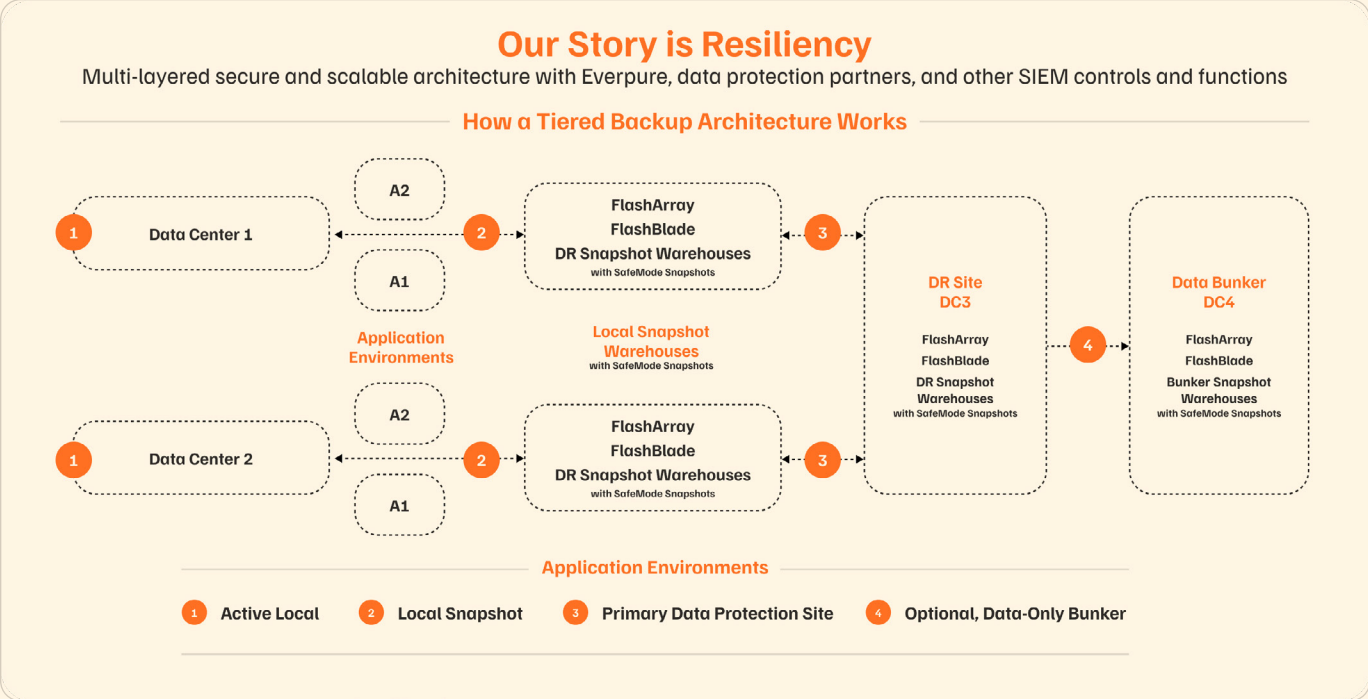

FIGURE 2 How a tiered backup architecture works

Other features and capabilities:

- System assessment and predictive support is simple with Pure1®. This cloud-based tool provides full-stack analytics, a data resilience score, and the AI-driven power of Pure1 Meta® to assess your environment's vulnerability and enable you to remediate weaknesses. With a single interface to manage all your storage arrays, Pure1 provides critical insights into your technology stack, including a topology view to simplify VM troubleshooting.
- The Purity ActiveCluster™ solution makes the highest levels of availability easy and affordable. With ActiveCluster, zero recovery point objective (RPO) and recovery time objective (RTO) between FlashArray systems can be achieved with true active-active synchronous replication for transparent failover.
- Everpure Cloud enables cloud-native block storage for seamless data mobility across on-premises and cloud environments while protecting cloud data and delivering fast RTOs and RPOs. Its always-on encryption and cloud-native cybersecurity provides a solution that safeguards data and supports compliance with regulatory and industry requirements while preserving data integrity and supporting continuous uptime.
- Pure Protect® //DRaaS is a disaster recovery as-a-service solution that reduces complexity, cost, recovery time, and business disruption following disasters and cyber disruptions. Firms now have clean environments with multiple restore points to recover clean copies of their on-premises vSphere data, to native AWS EC2, no matter what underlying storage infrastructure it is, while ensuring data centers remain isolated for investigation.
- A ransomware recovery SLA for as-a-service offering that is unique within the storage industry and a Zero Data Loss Guarantee across the Evergreen portfolio offering peace of mind that customer data will not be lost due to Everpure hardware or software issues.

> “With billions of dollars at stake and their reputations on the line if systems go down, our clients need reliable, secure data services. That’s exactly what Everpure enables us to deliver, positioning us to build strong client relationships for the long term.”
>
> **JESSE BONSERIO, SENIOR DIRECTOR OF ENGINEERING, ABACUS GROUP[7]**

Flash media solutions are ideal for operational resilience because they totally change the way we address data agility across silos. Flash performance and reliability enables a new way of working that financial institutions can utilize to enhance operational resilience in ways that will also set them up to address future challenges—all at a competitive cost, even for cold data.

Conclusion: Maximizing operational resilience in financial services

Risk management for financial services is constantly evolving and it’s pretty clear that going forward operational resilience is going to be a big part of any risk management regime. Regulators across the globe have taken note of the fact that markets have never been more interconnected and that technology is an Achilles Heel[8] for the system as a whole. With the addition of comprehensive approaches like DORA, regulators have indicated that they are changing the way in which they view and manage risk. Financial services firms need to take heed and follow their lead.

Just as operational resilience begins with the notion that it’s a matter of “when, not if” disruptive events will occur, so too must financial institutions recognize that it’s also true that it’s “when, not if” regulators will demand ever greater requirements for operational resilience. And, at the same time, the cost of noncompliance—whether from fines, other costs, or loss of business due to reputational failures—will continue to increase as well.

The challenges are big and the path forward is both complex and evolving, making a game plan hard to discern, but the issue cannot be ignored. The best time to start is now, even if it is to take small steps to begin. At the end of the day, much will change and everything from people to processes will be affected. It’s time to get going.

Additional resources

Next steps

- Find out what a resilience architecture is and how to build one.
- Learn how Everpure data solutions accelerate financial services.
- Meet with an expert to help strengthen your operational resilience.

Supporting information

- Data protection
- Business continuity

Ransomware mitigation

1 | As Risks Intensify, CEOs Can View Operational Resilience as a Competitive Advantage
2 | BCBS Revisions to the Principles for the Sound Management of Operational Risk | PwC UK
3 | UK Financial Regulators Levy Nearly £50 Million in Fines for Bank’s Operational Resiliency Failures—Tech & Sourcing @ Morgan Lewis
4 | Meeting the Challenge of HKMA Operational Resilience Requirements
5 | PS21/3 Building operational resilience | FCA
6 | Operational Resilience: It’s a Global Issue
7 | Abacus Group Builds Trust in the Finance Industry | Everpure
8 | https://www.britishmuseum.org/blog/who-was-achilles

ID17046-01-en-03/26