White Paper

Building a Resilient Financial Services Infrastructure: Digital Operational Resilience Act (DORA) and Beyond

Practical considerations for Banking, Financial Services & Insurance (BFSI) infrastructure leaders facing new global operational resilience and security requirements.

NUTANIX

Table of Contents

The implementation of the European Union's Digital Operational Resilience Act (DORA) marks a pivotal shift in financial regulation. As of January 17, 2025, the focus for financial entities and critical information and communication technology (ICT) providers moves beyond traditional cybersecurity prevention to comprehensive Operational Resilience. DORA represents a significant evolution in the EU regulatory framework, elevating operational resilience to a level of importance comparable-within its domain-to the role that financial resilience reforms such as the Dodd-Frank Act played for systemically important institutions.

This regulatory evolution is not limited to the EU; it mirrors a global convergence of standards, from the UK's FCA requirements to new guidelines in the US and APAC (eg. Australia and Singapore), that prioritizes the ability to withstand, recover, and learn from ICT disruptions.

For executives and IT leaders, this requires a fundamental architectural rethink; a transformational opportunity. Compliance strategies must now account for concentration risk, portability, and rigorous incident reporting.

This paper outlines how the Nutanix Cloud Platform (NCP) can support financial institutions in addressing the technical and operational aspects of these resilience mandates.

Heightened Global Operational Resilience Requirements (DORA & Beyond)

When the EU originally proposed DORA in September 2020, it signaled a new era for the importance of operational resilience.

As a cornerstone of the EU digital finance strategy, DORA is designed to "consolidate and upgrade information and communication technology (ICT) risk requirements" across Banking, Financial Services and Insurance (BFSI) entities to facilitate firms' alignment with "a common set of standards to mitigate ICT risks."

DORA applies to a comprehensive range of over 20 types of financial entities, spanning banking, payments, investment services, insurance, and crypto-assets, as well as market infrastructures (such as trading venues and central counterparties). Crucially, the regulation also extends to ICT third-party service providers (including cloud platforms.) For the exhaustive list of regulated entities, see Article 2(1) of DORA.

Global Regulatory Convergence: A Unified Challenge

DORA is the most comprehensive operational resilience regime currently in force, but it is not the only one. Comparable requirements addressing third-party risk, incident reporting, and business continuity have been issued or are under development by regulators in the United Kingdom, the United States, Canada, and across Asia-Pacific. For multinational financial institutions, the challenge is no longer complying with regional rules in isolation, but architecting a resilient infrastructure standard that can satisfy expectations across jurisdictions.

The Shift from Cyber Defense to Operational Resilience

Regulators worldwide are aligning on a core principle: preventing attacks is no longer sufficient; institutions must demonstrate the ability to withstand and recover from them. This shift is reshaping industry priorities.

According to a LSEG's From regulation to resilience: How financial firms are evolving their cloud strategies executive global research, 84% of firms have modified their cloud strategies in response to data privacy, security and sovereignty regulations, with 28% making extensive changes. Operational resilience has emerged as a shared priority for both firms and regulators: 47% of institutions now cite resilience and security as a key performance indicator for evaluating their cloud strategies, particularly as 30% experienced cloud-related operational disruptions in the past year.

The European Regulatory Landscape: DORA and Adjacent Frameworks

DORA does not operate in isolation. It sits within a layered European framework where cross-sector and sector-specific regimes interact, and where adjacent developments shape the broader compliance environment.

It is important to distinguish between DORA's core mandates and the broader foundation and adjacent regimes that influence digital strategy.

Foundation Layer: Cross-Sector Requirements

While DORA is the primary focus for financial entities, it sits atop a broader European resilience architecture:

- **NIS2 (Network and Information Systems Directive 2)**: Establishes baseline cybersecurity requirements across all critical sectors. As lex specialis, DORA's specific requirements take precedence over NIS2 for financial institutions. However, NIS2 remains a relevant secondary framework for areas not explicitly covered by DORA's sectoral rules.
- **CER (Critical Entities Resilience Directive)**: Focuses on physical resilience (e.g., natural disasters and sabotage). Major financial institutions may fall under its scope, requiring a strategy that integrates both digital (DORA) and physical (CER) security.

Adjacent Developments to Monitor

Beyond DORA's core scope, two further regimes affect infrastructure and operational decisions for financial institutions and warrant tracking alongside DORA implementation rather than as part of it:

PSD3 & PSR (Payment Services Directive 3 & Payment Services Regulation): The evolution of PSD2 makes system resilience a licensing requirement for payment firms, with reinforced fraud protection and verification requirements. The resilience objectives align with DORA's direction of travel.

Cross-Cutting Principles also affect infrastructure decisions. These include data location, cross-border data transfer, and AI governance requirements. Under the **EU AI Act**, the bans on certain AI practices and the AI literacy obligations began applying on February 2, 2025. Most obligations for high-risk AI systems apply from August 2, 2026, with later dates for certain categories. High-risk use cases relevant to financial services include creditworthiness evaluation, insurance risk assessment, and fraud detection.

In the EMEA region, 95% of financial institutions rate operational resilience as very important or critical when selecting cloud providers, reflecting the maturity of the regulatory framework.

Regional Alignment with DORA Principles

Although specific frameworks vary, major financial markets are converging on requirements that mirror DORA's focus on third-party risk and business continuity:

United Kingdom Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA): Post-Brexit frameworks have remained closely aligned with EU standards, though through two distinct regimes that should not be conflated. The first is the UK's existing operational resilience framework, set out in FCA PS21/3 and the PRA's supervisory statement on impact tolerances. The transition period for firms to demonstrate they could remain within impact tolerances for severe but plausible disruptions ended on March 31, 2025. This regime emphasizes that firms must be capable of terminating outsourcing arrangements without compromising service continuity, a direct parallel to DORA's cloud exit strategy focus.

The second is a new reporting regime. On March 18, 2026, the FCA and PRA published final policy statements PS2/26 and PS7/26, establishing a unified approach to operational incident and material third-party reporting. These rules take effect on March 18, 2027, and introduce a single reporting portal (FCA Connect) with a streamlined template aligned with both DORA and the FSB's FIRE framework, an illustration of the global regulatory convergence underway.

North America

United States: Banking regulators (Federal Reserve, Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC)) have issued joint guidance strengthening expectations for operational resilience, particularly regarding third-party relationships.

Canada - Office of the Superintendent of Financial Institutions (OSFI): Canadian regulators have taken a comprehensive, phased approach, issuing three major guidelines: Third-Party Risk Management (April 2023), Integrity and Security (January 2024), and Operational Risk Management and Resilience (August 2024). This systematic approach has resulted in 96% of Canadian banks making moderate or extensive changes to their cloud strategies.

Asia-Pacific

The Asia-Pacific region is responding to high cloud-related disruption rates (38% in the past 12 months according to LSEG research).

Regulators in Singapore (Monetary Authority of Singapore, MAS), Hong Kong (Hong Kong Monetary Authority, HKMA), Australia (Australian Prudential Regulation Authority, APRA), and India (under the Digital Personal Data Protection Act, 2023) have updated guidelines to mandate stricter business continuity management.

Notably, in November 2024, eight jurisdictions conducted a joint crisis

management exercise with global cloud providers, signaling a new level of cross-border regulatory coordination.

The Strategic Implication

This global convergence signals that operational resilience, third-party risk management, and digital sovereignty are no longer regional compliance tasks but global strategic imperatives. Financial institutions that treat these regulations as a unified architectural challenge, rather than a checklist of local rules, can build a "future-proof" foundation that supports business agility across all jurisdictions.

Understanding DORA's Impact

The Digital Operational Resilience Act (DORA) is structured around five key pillars designed to strengthen the financial sector's defense against ICT disruptions. Together, these pillars establish a comprehensive framework covering how financial entities govern ICT risk, manage and report incidents, test their resilience, oversee third-party providers, and share intelligence on emerging threats:

- ICT Risk Management: the governance, policies, and controls firms must put in place to identify, protect against, and recover from ICT risks.
- ICT-Related Incident Management, Classification, and Reporting: standardized processes for detecting, classifying, and reporting major ICT incidents to regulators.
- Digital Operational Resilience Testing: regular testing of ICT systems, including threat-led penetration testing for significant entities.
- ICT Third-Party Risk Management: oversight of ICT service providers, with heightened requirements for critical third parties subject to direct EU supervision.
- Information and Intelligence Sharing: voluntary arrangements among financial entities to exchange cyber threat information and intelligence.

While DORA comprises a broad set of governance rules, its successful implementation relies heavily on the underlying technical infrastructure. The figure below illustrates how DORA structures its requirements across five distinct, comprehensive chapters that are widely recognized as its core pillars. These five pillars, and the framework that follows maps DORA's core requirements to specific Nutanix Cloud Platform capabilities, demonstrating how infrastructure choices can support broader compliance objectives.

The following framework maps DORA's core requirements to specific Nutanix Cloud Platform capabilities, demonstrating how infrastructure choices can support broader compliance objectives.

Figure 1: DORA pillars

Pillar 1: ICT risk management

The Regulatory Goal: Establish a comprehensive framework for the management of ICT risk, including resilient systems, protection mechanisms, and the segregation of critical functions

DORA Focus Area (The Regulation)	Nutanix Capability (Solution)
Governance & Visibility (Article 6): Unified management of all physical and digital infrastructure (On-prem/Cloud). Article. 28(3): Comprehensive inventory of ICT third-party arrangements supporting ongoing register maintenance and the annual reporting cycle. Per Article 6(8), the ICT risk management framework must include "all relevant physical components and infrastructures, such as premises, datacenters, and sensitive designated areas."	**Unified Control Plane:** To help support these requirements, the Nutanix Cloud Manager (NCM) solution offers a centralized interface designed to assist teams in maintaining visibility across disparate environments.
Technological Resilience (Article 7) Systems must demonstrate reliability and data integrity.	**Self-Healing Architecture:** The Nutanix Acropolis Operating System (AOS) utilizes distributed consistency algorithms to help protect data availability against hardware or node failures.
Protection & Prevention (Article 9, Article 10, Article 11) Implement prevention and protection tools, detection mechanisms, and robust response, recovery, and business continuity plans for ICT systems.	**Integrated Defense:** Native capabilities such as Nutanix Data Lens (ransomware detection) and Nutanix Flow Network Security (microsegmentation) can support a defense-in-depth security posture aligned with regulatory expectations. Nutanix's ecosystem of partner companies offers multiple prevention, protection, detection, and response capabilities.
System Segregation (Article 12) ICT systems should be logically or physically segregated to mitigate the risk of lateral movement and corruption. Per Article 12, ICT systems: "shall be securely protected from any unauthorized access or ICT corruption and allow for the timely restoration of services, making use of data and system backups as necessary."	**Zero Trust Segmentation:** Flow Network Security can be used to implement microsegmentation strategies that can help isolate critical applications. **Hybrid Multicloud Portability:** Nutanix Cloud Clusters (NC2) enables organizations to create isolated recovery environments, which can support resilience and recovery strategies in multiple public clouds, at the edge and on-premise. **Application Resilience:** Nutanix Kubernetes Platform (NKP) extends segmentation to the containerized layer using standard Kubernetes network policies. NKP also offers hybrid multicloud multitenancy with dedicated or shared Kubernetes clusters to support deployment models that may help address certain regulatory and operational requirements.

Pillars 2 and 3: Incident Reporting & Operational Testing

The Regulatory Goal: Financial entities must demonstrate the ability to detect anomalies rapidly, report incidents within prescribed timelines, and continuously test systems without disrupting production. These pillars cover continuous monitoring, timely detection and classification of ICT incidents, structured reporting to regulators, and regular testing of systems to validate resilience under both normal and stressed conditions, including obligations under Article 10 (detection) and Articles 17 through 23 (incident management, classification, and reporting).

The Nutanix capabilities described below can assist institutions in addressing certain technical aspects of these obligations, for example, by generating evidence and supporting workflows that contribute to incident detection and reporting processes.

- **Continuous Monitoring (Day 2 Operations):** DORA emphasizes ongoing maintenance and "Day 2" operational excellence. Nutanix provides real-time monitoring and anomaly detection across the IT estate, generating the security logs, network traffic data, and consolidated evidence base that contribute to incident detection and reporting processes.
- **Automated Response:** Manual processes are often insufficient to meet internal and regulatory reporting timelines. Nutanix X-Play (part of NCM) enables automated remediation workflows, allowing IT teams to operationalize their incident response playbooks.
- **Non-Disruptive Testing:** Regular resilience testing often disrupts business. The Nutanix platform supports non-disruptive upgrades and testing, allowing organizations to validate aspects of their resilience posture without maintenance windows.

Pillar 4: Third-Party Risk Management

The Regulatory Goal: Reduce concentration risk and support sound "exit strategies" for critical third-party ICT providers (e.g., cloud hyperscalers).

- **Addressing Concentration Risk (Article 31):** Financial entities are increasingly subject to requirements to demonstrate that critical functions are not solely dependent on a single provider and maintain the capability to transition workloads if necessary. The Nutanix Cloud Platform architecture abstracts underlying hardware and cloud layers, which can facilitate a hybrid multicloud operating model and support strategies aimed at mitigating concentration risk.

This regulatory requirement is no longer hypothetical. In November 2025, European Supervisory Authorities (ESAs) designated the first group of Critical ICT Third-Party Providers (CTPPs) under the DORA Article 31. The designated providers, which include major hyperscalers and infrastructure firms, are now

subject to direct regulatory oversight, including risk assessments and inspections by Joint Examination Teams. For financial entities utilizing these designated providers, Nutanix Cloud Clusters (NC2) and the Nutanix Move solution can support workload portability and concentration risk mitigation strategies.

DORA Third-Party Exit Strategy Requirements

Under DORA Article 28(8), financial entities must have exit strategies in place for ICT services supporting critical or important functions. These requirements apply to all ICT third-party service providers, including cloud service providers, and align with prior European Banking Authority (EBA) Guidelines on Outsourcing Arrangements (EBA/GL/2019/02, paragraphs 105–106). For cloud-based services, this requirement carries particular operational weight given concentration risk and portability challenges.

- **Enabling the Exit Strategy (Article 28):** A credible exit strategy requires technical portability, not just contractual clauses. By utilizing Nutanix Cloud Clusters (NC2) and Nutanix Move, organizations can port workloads between on-premises datacenters and public clouds, supporting technical portability as one component of a broader multi-provider and exit strategy.

Pillar 5: Information Sharing

The Regulatory Goal: Facilitate the exchange of cyber threat information and intelligence among financial entities.

Intelligence Integration: Effective sharing requires clean, accessible data. Nutanix operates as an open platform with comprehensive APIs, serving as a reliable data source for SIEMs (Security Information and Event Management) and SOARs (Security Orchestration, Automation and Response), including platforms such as Splunk. This integration can provide data inputs that support threat intelligence sharing across existing security and information-sharing frameworks.

Nutanix Solutions for Resilience and Security

The Nutanix platform is designed to assist financial institutions in enhancing, hardening, and protecting their environments. By integrating security and resilience directly into the infrastructure stack, Nutanix supports a “Secure by Design” approach that aligns with key regulatory principles, including those reflected in DORA.

1. Hybrid Multicloud Architecture & Workload Mobility

Regulators increasingly emphasize the ability to move critical workloads as part of concentration risk mitigation strategies. The Nutanix capabilities below can assist institutions in addressing certain technical aspects of workload portability:

- **Unified Infrastructure:** Nutanix Cloud Clusters (NC2) enables customers to relocate workloads from on-premises locations to public clouds without refactoring. This diversity can support resilience objectives and simplifies migration between providers.
- **Streamlined Migration:** Nutanix Move facilitates the re-platforming of virtual machines, allowing migrations to be scheduled or run on-demand to support cloud exit strategies.
- **Container Portability:** For cloud-native applications, the Nutanix Kubernetes Platform (NKP) provides a consistent operating model based on upstream Kubernetes. This helps containerized applications remain portable across diverse environments.

2. Operational Resilience, Cyber & Zero Trust Strategy

Nutanix is purpose-built to support infrastructure resilience across diverse environments, including core datacenters, edge locations, and public clouds. This architecture allows organizations to apply consistent security and business continuity policies across all endpoints, supporting a comprehensive resilience posture. To further harden these environments, Nutanix incorporates Zero Trust principles, such as microsegmentation and rigorous access controls, directly into the platform, enabling customers to implement controls aimed at restricting lateral movement and reducing the attack surface.

- **Self-Healing Infrastructure:** Nutanix Cloud Infrastructure (NCI) manages storage resources to help mitigate certain infrastructure-level risks to data and system integrity in the event of an attack that targets a node, disk, or software failure. NCI does this through tunable redundancy, cluster fault tolerance, creation of availability domains for block- and rack-aware fault tolerance, and data path resilience. NCI also provides automated detection of degradation, and includes failure recovery capabilities to assist in maintaining availability during attacks or outages.

- **Integrated network security:** Nutanix Cloud Infrastructure (NCI) delivers automated networking with Nutanix Flow Network Security, creating software-based firewalls to segment critical apps and data without the management overhead of traditional appliances.
- **Continuous Monitoring:** Nutanix Security Central assists with inventory, threat detection, and compliance tracking. Assets and their configuration are tracked over time in a cloud-based portal to detect changes and track compliance with best practices. Network traffic data is analyzed for unusual behavior to generate threat detection alerts of unusual access patterns. Automated reporting makes configuration, compliance, and threat data available on a regular basis for tracking over time.
- **Hybrid cloud SecOps solutions**
  - Robust unified network and applications monitoring with Nutanix AHV hypervisor and Flow solutions.
  - Centralized management with Prism Control.
  - Mitigate vulnerability exploits: Monitor VM vulnerabilities and prioritize patching. Qualys integration with Nutanix Security Central.
  - Centralized SIEM Integration for Continuous Monitoring.
  - Control lateral movement: Automate flow and microsegmentation policy creation, ML-based analysis, and planning to identify and recommend policy changes.
- **Ecosystem interoperability**
  - 200+ Nutanix Ready partner security solutions deliver quick time to value (SIEM and UEBA integrations, threat intel, EDR/NDR).
  - Integration with existing vendor stack.
  - API first approach.
  - See Nutanix's reference architecture: Agile Security and Ops with Well-Architected Splunk on Nutanix - SIEM and SOAR Solutions.

3. Data Protection & Ransomware Defense

To address the threat of data breaches and ransomware, Nutanix provides tools for lifecycle management of data backup and recovery.

- **Ransomware Containment:** Nutanix Unified Storage (NUS) and Nutanix Data Lens (NDL) provide analytics to help monitor, detect, and respond to potential ransomware activity and operationalize a recovery strategy for cyber-attacks.
- **Immutable Recovery:** The platform enables natively integrated snapshots, replication, and DR services such as Write Once Read Many (WORM) for immutable backups, secure snapshots, and self-service restore capabilities to support data protection and recovery strategies.

  - Further, Nutanix MST (Multicloud Snapshot Technology) allows customers to distribute, manage and restore snapshots across hybrid multicloud endpoints.
- **Geographic Redundancy:** Nutanix Business Continuity and Disaster Recovery (BCDR) provides backup capabilities and rapid restore functionality that can support recovery from breaches and outages. Data can be replicated to two alternative geographical locations, which can assist institutions in addressing certain technical aspects of business continuity objectives even if two sites have been compromised.
- **Kubernetes Protection:** Nutanix Data Services for Kubernetes (NDK) extends these protections to stateful containerized applications, enabling policy-driven disaster recovery.

4. Operational Governance & Ecosystem Integration

Resilience requires visibility. Nutanix facilitates compliance adherence through unified management and a robust partner ecosystem.

- **Unified Control Plane:** Nutanix Cloud Manager (NCM) enables hybrid multicloud orchestration to automate the provisioning of hybrid cloud architectures and manage multi-tiered and distributed applications across different cloud environments from a single control plane. NCM provides the capabilities for holistic security monitoring, remediation, and asset visibility across multiple clouds.
- **Database Management:** Nutanix Database-as-a-Service streamlines the patching and scaling of major databases (SQL Server, Oracle, PostgreSQL and MongoDB), utilizing role-based access controls (RBAC) to support compliance and consistency.
- **Ecosystem Interoperability:** An API-first approach allows deep integration with over 200 “Nutanix Ready” security partners. This includes centralized SIEM integration for continuous monitoring and automated response workflows with platforms like Splunk.
- **Secure Remote Work:** For end-user computing, VDI and DaaS solutions provide robust, identity-based access policies to secure remote workspaces.

The Trusted Ecosystem

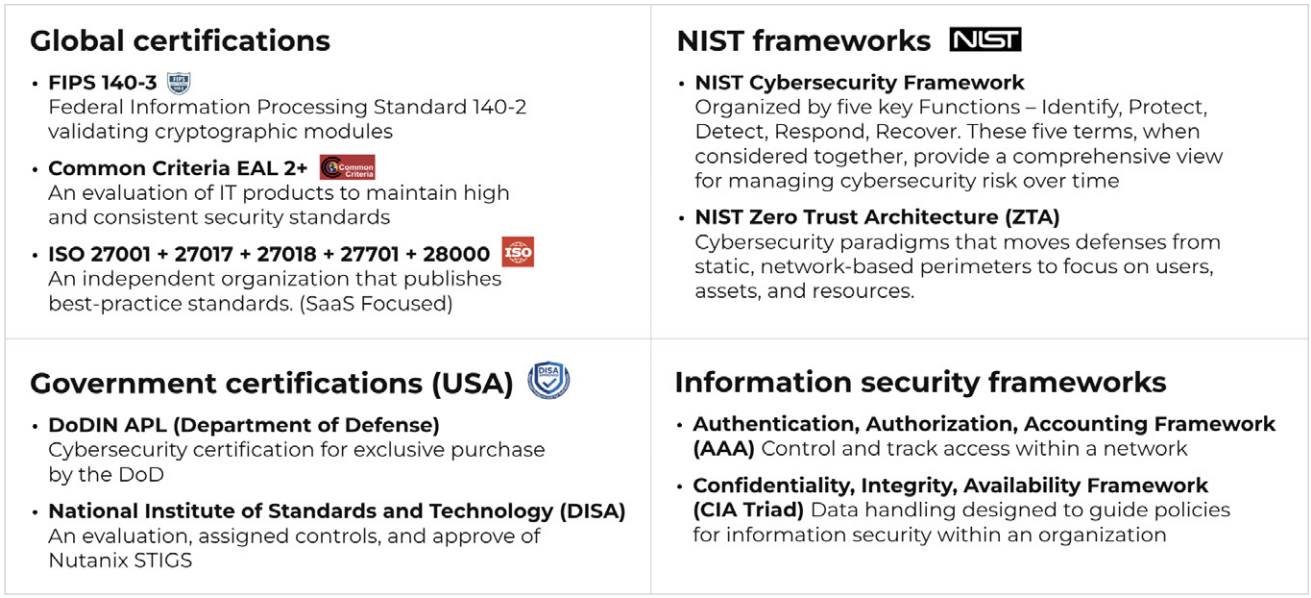
Building on a Foundation of Validated Trust

Operational resilience requires more than just robust software; it demands a verifiable chain of trust. The Nutanix Cloud Platform is engineered with reference to widely recognized security and compliance standards used in the financial industry. This security posture is supported through extensive third-party audits and alignment with international frameworks, providing a platform that can assist financial institutions in addressing certain technical aspects of their assurance needs when hosting critical workloads.

Certifications and Standards Alignment

Nutanix maintains a comprehensive portfolio of security validations that support global regulatory compliance efforts.

Figure 2: Nutanix compliance and frameworks alignment



https://www.nutanix.com/trust

Cybersecurity

NCP enables a unified, layered approach to cybersecurity across its platform, data, networks, and applications. Together, this helps build strong cyber resilience in the face of constant threats. Aligned to the NIST Cybersecurity Framework (NIST CSF), NCP provides built-in capabilities.

Figure 3: Nutanix Approach to Simplifying Security

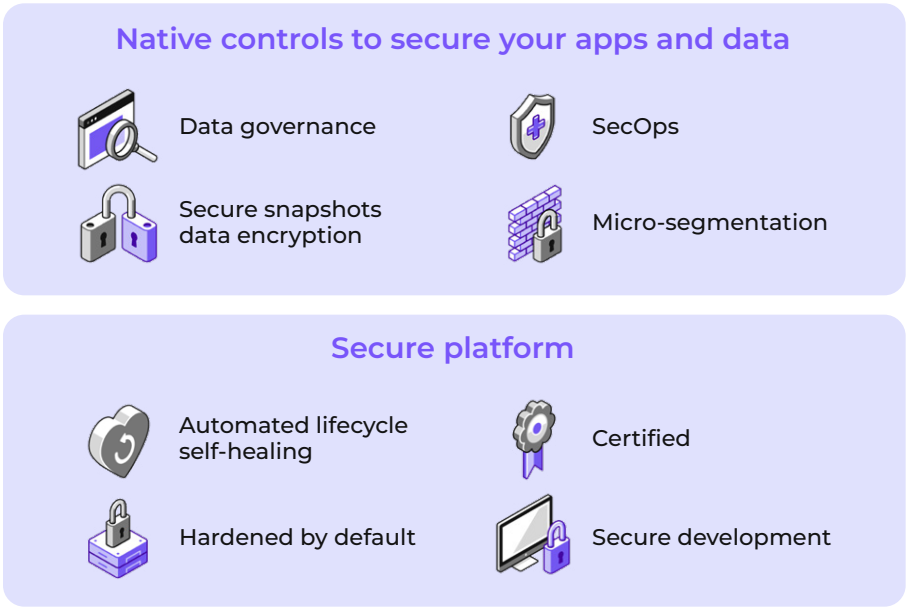
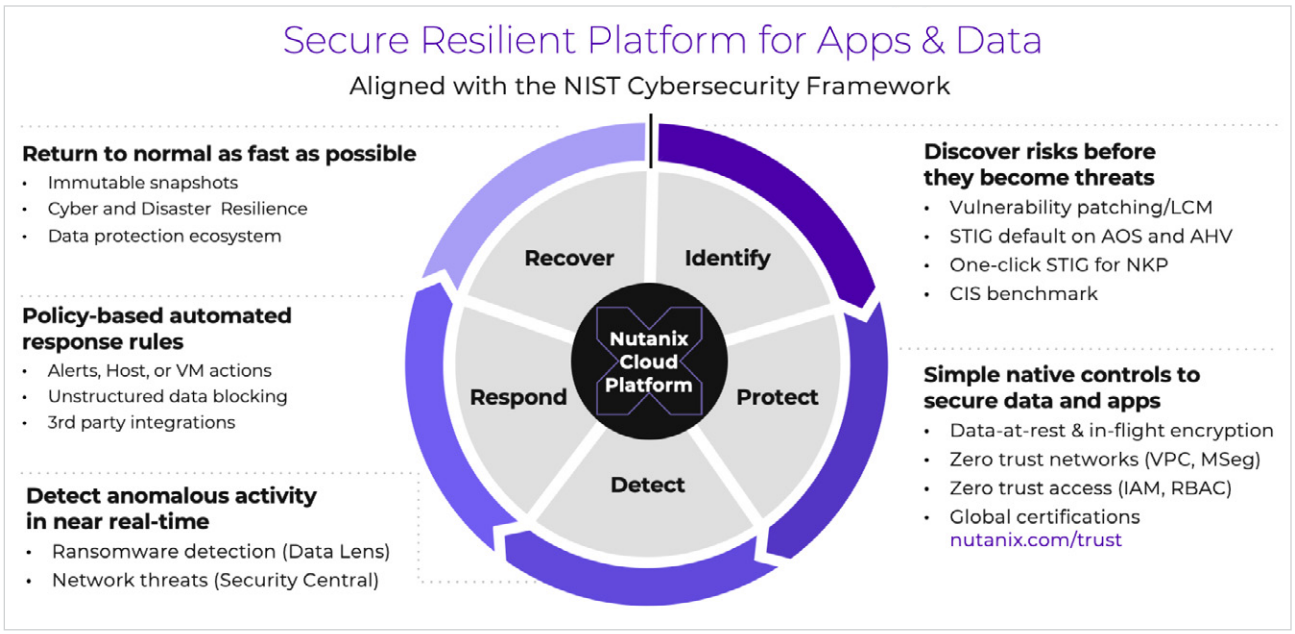


Figure 4: Nutanix NIST Cybersecurity Framework Alignment

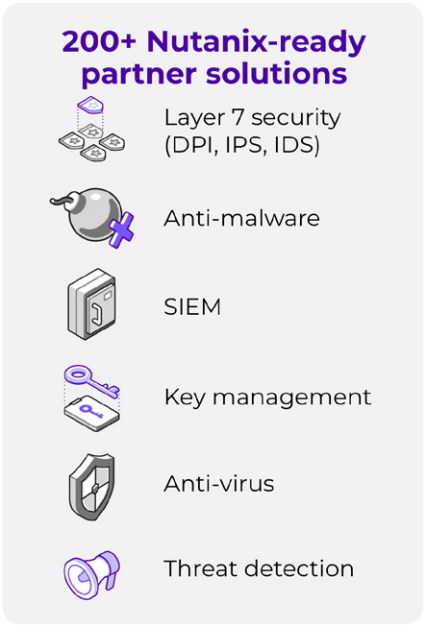


Defense-in-Depth: The Partner Ecosystem

Resilience is a team sport. Rather than displacing existing security investments, Nutanix integrates with an extensive ecosystem of certified "Nutanix Ready" security and data protection partners spanning the full defense-in-depth stack: endpoint detection and response, network security and microsegmentation, data protection and backup, identity and access management, SIEM and observability, and cloud workload protection. This allows financial institutions to operationalize their existing security tooling directly within the infrastructure layer, preserving prior investments while extending coverage uniformly across virtual and multi-cloud environments. A current list of certified partners is maintained in the Nutanix Ready partner directory.

Next-generation and critical workloads for Nutanix Customers

Our hybrid multicloud platform supports a wide array of business use cases. Nutanix balances workload placement, resilience, performance, costs, and control factors for modern and business-critical applications such as core banking, risk management, OMS/EMS, and SWIFT. Nutanix can support a BFSI's microservices management to give developers and IT simplified IaaS (Infrastructure as a Service) choices.



Future Proofing with Nutanix

DORA elevates ICT risk management to a sustained board-level priority, and it is not alone. The convergence underway across the United Kingdom, United States, Canada, and Asia-Pacific means that financial institutions are no longer responding to a single regulation but to a unifying set of expectations on operational resilience, third-party risk management, and digital sovereignty. What began as a regional compliance exercise is becoming a global architectural conversation.

For multinational institutions, this shift changes the calculus. Building one resilience posture per jurisdiction is neither sustainable nor strategic. The institutions that fare best will be those that treat resilience, portability, and observability as platform-level properties, applied consistently across geographies, providers, and workload types, rather than as point solutions bolted onto each new regulatory deadline.

Addressing these requirements is not a one-time exercise but a continuous journey of modernization. Financial institutions need infrastructure that offers inherent resilience without stifling innovation, and that can flex as regulations evolve and business needs change.

By standardizing on the Nutanix Cloud Platform, BFSIs are better positioned to:

- **Support strategies aimed at mitigating concentration risk:** Leverage portable licensing and workloads to move data and applications between

on-premises environments and public clouds, supporting the exit-strategy expectations now common across DORA, UK FCA/PRA guidance, US joint regulator guidance, and OSFI's third-party risk framework.

- **Enhance operational continuity capabilities:** Utilize built-in redundancy and automated disaster recovery to help maintain critical functions during disruptions, regardless of where workloads run.
- **Support centralized visibility and reporting processes:** Centralize visibility across hybrid environments to assist institutions in addressing the transparency, monitoring, and information-sharing themes shared across DORA and the converging global regimes.

Nutanix offers a pragmatic path forward, helping financial institutions modernize their digital estates to meet today's resilience standards under DORA and the converging global frameworks that surround it, while preparing for the regulatory demands of tomorrow.

Regulatory Compliance & Infrastructure Disclaimer

This document is provided for informational purposes only. Nutanix provides the underlying infrastructure, platforms, and technical tools designed to facilitate a resilient digital environment; however, Nutanix does not provide legal, regulatory, or compliance advice.

While the Nutanix Cloud Platform (NCP) includes features that can support certain technical and operational aspects of regulatory requirements, including the Digital Operational Resilience Act (DORA), customers remain responsible for assessing and ensuring that their specific implementation meets applicable legal and regulatory requirements. In particular, customers are responsible for:

- **Regulatory Alignment:** Determining whether and how their use of Nutanix solutions complies with applicable laws and regulations, including the UK's FCA/PRA requirements, US banking guidance (Federal Reserve, OCC, FDIC), and Canada's OSFI guidelines.
- **Compliance Outcomes:** Achieving and maintaining compliance with all applicable laws and regulations. Nutanix products and services do not, in themselves, ensure or guarantee compliance with any regulatory framework.
- **Policy Governance:** Designing, implementing, and maintaining appropriate governance frameworks, including ICT risk management, incident management and reporting processes, operational resilience testing, and third-party risk management and exit strategies.

Specific Note on DORA and Global Mandates

The implementation of DORA marks a shift toward comprehensive Operational Resilience. While Nutanix provides technical capabilities like workload portability (via NC2) and microsegmentation (via Flow Network Security) that can help mitigate certain ICT risks, these are components of a broader compliance strategy that extends beyond underlying infrastructure and must be implemented and managed by the financial institution.

Compliance with DORA requires financial institutions to implement governance, oversight, testing, documentation, incident classification and reporting, and third-party risk management processes.

Accordingly, references in this document to "alignment" or "support" relate to technical capabilities only and should be evaluated by the customer in the context of its overall legal and regulatory obligations. Nothing in this document should be construed as a representation or warranty of regulatory compliance.

PSM-Building-a-Resilient-Financial-Services-Infrastructure-White-Paper-FY26Q3