restorepoint
A ScienceLogic company

SOLUTION BRIEF

Operational Resilience: Complying with New and Changing Rules for Network Management

Proper network management is of vital importance to the CIOs and CISOs tasked with keeping enterprise systems and data available, efficient, and safe. And more than merely a business imperative, maintaining secure and resilient technology operations has been identified as an issue of strategic national economic security to protect critical infrastructure, digital supply chains, patient health and safety, and the flow of trillions of dollars in commerce each year.

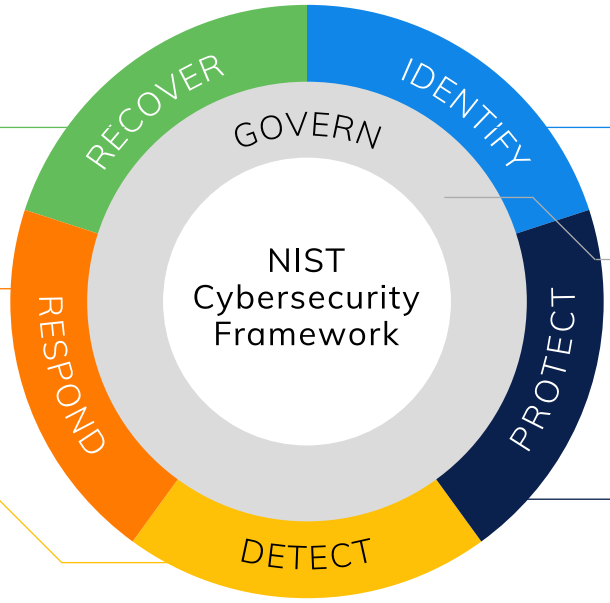
To ensure that organizations are all on the same page in building and managing systems that work well together, many industry and international standards bodies have articulated operational frameworks to support the goals of resiliency and security. Some examples include the U.S. National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF 2.0), the International Organization for Standardization's (ISO) ISO/IEC 27001 for information security management systems, and the Basel Committee on Banking Supervision's Principles for Operational Resilience.

NIST CSF 2.0 identifies six foundational pillars for building and maintaining networks that are resilient and secure, namely:

Recover
Ensure that any disruptions are corrected and downtime is minimized.

Respond
Be able to act quickly to stop, contain, and mitigate an attack or incident.

Detect
Have the capacity to determine when an attack or disruption has occurred.



Identify
Establish the means to discover all elements of the network.

Govern
Provide the means to manage a network and its controls effectively and efficiently.

Protect
Deploy tools and safeguards for keeping systems and data safe.

What is Operational Resilience?

Fundamental to operations resilience is the ability to provide uninterrupted, mission-critical services even in the face of natural disasters, geopolitical conflict, cyberattacks, or technical errors in the event of disruptions. Doing this depends on the stability and availability of an organization's network, or **operational resilience**. We like the Bank of England's definition of the term:

"The ability of firms, and the financial sector as a whole, to absorb and adapt to shocks and disruptions, rather than contribute to them."

Why is Operational Resilience Important?

Customers, partners, and users expect 24x7 availability of IT services, and they rely on organizations, agencies, service providers, and other third parties to keep their assets, data, and identities secure. And those third parties must be able to communicate and interact with their digital supply chains. Doing all this requires excellence in network management including monitoring network components and performance, combating cyber threats, backing up configurations for key network devices, and enabling the swift recovery of network infrastructure after a disruption. These are vital aspects of ensuring operational resilience and security. Furthermore, all these goals must be met while maintaining strict compliance under a complex of industry, national, and international standards and regulations.

Standards and Regulations

Although not exhaustive, the following are some of the major security and resilience standards and regulations from around the world:

Country	Standard / Rule
Australia	APRA CPS 230
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)
EU	EU Digital Operational Resilience Act (DORA)
EU	General Data Privacy Regulation (GDPR)
EU	Payment Services Directive 2 (PSD2)
Hong Kong	Supervisory Policy Manual—Operational Resilience
Luxembourg	CSSF 21/787 Major Incident Reporting
Singapore	Guidelines on Business Continuity Management
South Africa	D4-2023 Directive on Operational Resilience
Switzerland	FINMA Circular 2023/1 Operational risks and resilience
UAE	DFSA AMI 5.5
UK	Data Protection Act (DPA)
UK	Financial Conduct Authority SYS 15A.2
US	Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers
US	Gramm-Leach-Bliley Act (GLBA)
US	Banking Secrecy Act (BSA)
US	Federal Financial Institutions Examination Council (FFIEC) Guidelines
US	NIST Cybersecurity Framework
US	Sarbanes-Oxley (SOX)
Industry Standard	Payment Card Industry Digital Security Standard (PCI DSS)

Consequences of Operational Non-Resilience

According to the Ponemon Institute/IBM **2023 Cost of a Data Breach Report**, organizations that suffer a data breach can expect to lose $4.45 million for an incident in which personal or regulated data is compromised. Depending on circumstances, some events can be much more.

Under GDPR in the EU, for example, fines alone may be €20 million or 4% of a firm's annual revenue, whichever amount is higher. Total costs for a non-compliance include factors like:

Fines and penalties levied by government regulators and industry bodies.

Costs associated with legal and consulting fees, technical investigations, recovery, and necessary system upgrades.

Increased customer churn due to loss and brand trust and reputation.

Revenues lost due to lack of service availability.

Higher costs associated with new customer acquisition.

Solutions for Improving Operational Resilience

Achieving operational resilience means focusing on building a robust, available IT infrastructure and providing IT operations with tools designed to keep service delivery within established tolerances, identify and respond to malfunctions and software errors, and detect and prevent cyber-attacks.

Process automation is a key component to any tool designed to support IT management. Process automation ensures fast, accurate execution and contributes to lowering the costs associated with manual tasks. Vital processes that can and should be automated include:

Network monitoring across on-premises, cloud, and hybrid infrastructures

System backup and disaster recovery

Root cause analysis and incident response and remediation

Predictive analysis and maintenance

Configuration assessments and audits

CMDB update and synchronization

Compliance and health checks

Change management

ScienceLogic helps today's enterprise improve operational resilience and achieve regulatory compliance through its portfolio of IT Operations and Network Automation solutions.

ScienceLogic's Restorepoint solution enables our customers to dramatically reduce audit effort, improve availability, and meet required standards by automating critical network processes.

Combined with ScienceLogic SL1, your teams can see everything across multi-cloud and distributed architectures, contextualize data through relationship mapping, and act on this insight through integration and automation.

Contact us to learn how you can achieve operational resilience across your IT estate.