ScienceLogic

SOLUTION BRIEF

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

Effective network management is vital for CIOs and CISOs charged with keeping enterprise systems and data available, efficient, and secure. Beyond business imperative, resilient technology operations are now recognized as a matter of strategic national economic security—essential to protecting critical infrastructure, digital supply chains, patient health and safety, and the flow of trillions of dollars in commerce each year.

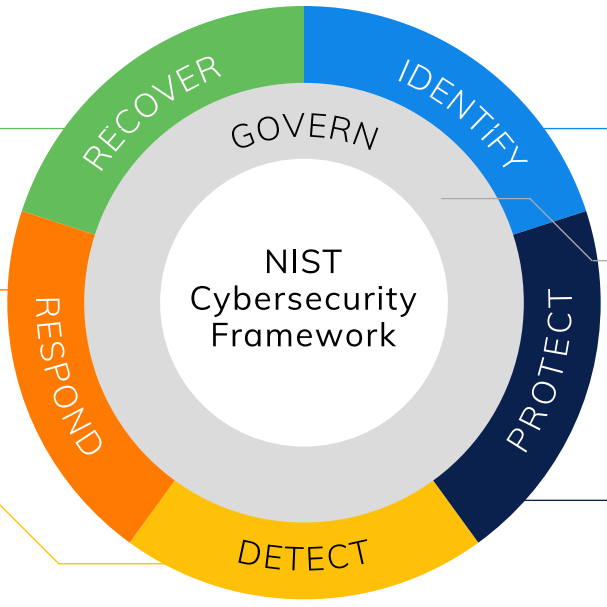
To ensure organizations are aligned in building and managing interoperable systems, many industry and international standards bodies have established operational frameworks that advance resiliency and security. Examples include the U.S. National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF 2.0), the International Organization for Standardization's (ISO) ISO/IEC 27001 for information security management, and the Basel Committee on Banking Supervision's Principles for Operational Resilience.

NIST CSF 2.0 defines six foundational pillars for building and sustaining resilient, secure networks:

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?

Operational resilience is the ability to deliver uninterrupted, mission-critical services even when facing natural disasters, geopolitical conflict, cyberattacks, or technical disruptions. It rests on the stability and availability of an organization's network.

NIST defines it as:

"Resilience is the ability of an information system to continue to (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs."

Why is Operational Resilience Important?

Customers, partners, and users expect always-available IT services and secure handling of their assets, data, and identities. To meet these expectations, organizations and their third-party providers must also ensure resilience across the digital supply chain.

Achieving this requires excellence in network management — monitoring performance, defending against cyber threats, backing up key device configurations, and enabling swift recovery of infrastructure after a disruption. These practices are essential to maintaining both operational resilience and security. At the same time, organizations must uphold strict compliance with a complex web of industry, national, and international regulations. 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

The following represent some of the most widely recognized security and resilience standards and regulations worldwide (not an exhaustive list):

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

Country	Standard / Rule
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 2025 Cost of a Data Breach Report, the average cost of a data breach reached $4.45 million per incident when personal or regulated data was compromised — with some events costing far more. Under the EU's GDPR, fines alone can be up to €20 million or 4% of annual revenue, whichever is higher. Total costs of non-compliance and service disruption can include:

- Fines and penalties levied by government regulators and industry bodies.
- Lost revenue from service availability.
- Legal, consulting, investigation, recovery, and necessary system upgrade expenses.
- Increased customer acquisition costs.
- Higher customer churn due to loss and reputational damage.

Solutions for Improving Operational Resilience

Operational resilience requires a robust IT infrastructure and operations teams equipped with tools that ensure service delivery, detect and respond to malfunctions, and defend against cyberattacks.

Process automation is central to this effort — enabling fast, accurate execution while reducing the costs and risks of manual work. Critical processes to automate include:

- Network observability across on-premises, cloud, and hybrid infrastructures
- System backup and disaster recovery
- Compliance and health checks
- Change management
- Predictive analysis and maintenance
- CMDB updates and synchronization
- Incident response and remediation
- Configuration assessment

ScienceLogic helps enterprises strengthen operational resilience and achieve regulatory compliance through its autonomic IT solutions.

skylar™ compliance

Skylar Compliance (formerly Restorepoint) reduces audit effort, improves availability, and ensures standards are met by automating critical network processes.

skylar™ one

Skylar One (formerly SL1) provides end-to-end visibility across multi-cloud and distributed architectures, contextualizes data through relationship mapping, and drives action through intelligent automation.

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