ScienceLogic

CHECKLIST

Checklist for Cyber Resilience

Cyber resilience is a critical issue for organizations because it is focused on maintaining business operations - and therefore revenue - through the preservation of operational integrity and security of the IT estate, minimizing the impact of cyber attacks, outages and human error. Cyber resilience has emerged as a mandate under several industry and regulatory regimes—the consequences for non-compliance during an incident are significant. Not only are non-compliance costs high for the organization, but there is a *legal precedent* for holding individual executives personally liable for incidents.

Therefore, understanding the requirements for achieving cyber resilience is important for anyone involved in IT-dependent services delivery. Economic security, public health and safety, and the delivery of goods and services depend on it.

That's why cyber resilience has been elevated to a matter of national strategic concern for most countries. The U.S. Cybersecurity Infrastructure and Security Agency (CISA) have identified *16 "critical infrastructure" industry sectors* for which cyber resilience must be achieved under its Critical Infrastructure Security and Resilience program.

For that reason, the U.S. National Institute of Standards and Technology (NIST) Computer Security Resource Center has published *NIST SP 800-160 Vol. 2 Rev. 1*: Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, to help organizations draft cyber resiliency strategies based on proven best practices.

The NIST framework is based on four goals:

- **Anticipate** and prepare for likely scenarios that challenge operational integrity;
- **Withstand** events that threaten operational integrity;
- **Recover** quickly from incidents that disrupt operations; and,
- **Adapt** based on lessons learned from adverse experiences

The task for organizations is in aligning these security goals with their unique operational characteristics, including things like industry-specific standards and regulations, IT infrastructure architecture, assets and configuration, risk tolerance, and mission/objectives.

Fortunately, there are tools available to help organizations achieve these goals by monitoring IT infrastructure, analyzing and auditing performance and settings, mitigating damage and restoring systems affected by outages and attacks, and applying new insights to improve policy and process.

To determine what's right for your organization requires understanding your organization's needs, setting objectives, and aligning priorities with capabilities.

Questions to ask before you start

To properly identify and set priorities for achieving operational resilience means obtaining stakeholder input to assess and quantify risk

Is IT operations mapped, monitored, and managed to support and prioritize service viability?

Everything runs through IT. Complete network topography, observability, and operational data collection supports preventive maintenance and rapid incident response, diagnostics, and recovery.

Do we have a backup strategy, including data and network configurations, and is it automated?

The Uptime Institute says 49% of all service outages are attributed to configuration and change management errors, and Gartner says outages cost $5,600 per minute.

What is our disaster recovery plan, and do we test and update it regularly?

The British Chamber of Commerce found 93% of organizations that suffer a major data loss event file for bankruptcy within a year.

How are our compliance obligations being managed, and are we capturing the data necessary for an audit?

Risk and compliance consultants Wolters Kluwer reports five major benefits from maintaining strong internal data capture practices: better risk management, greater assurance, enhanced efficiency, clearer reporting, and improved audit quality.

What is our worst-case scenario, and do we have a response contingency plan?

An erroneous code update knocked a major telco offline for 20 hours, affecting business, residential, and government services including 911 emergency services. Short-term recovery costs ran $150 million; long-term costs were expected to be $10 billion or more.

Setting Objectives

Once you've gained stakeholder consensus for setting priorities, you can establish program objectives. Here are some that align with operational resilience.

- ☑ **Identify important business services**. These are services that, if disrupted, could cause intolerable harm to operations.
- ☑ **Establish impact tolerances**. Impact tolerances define a threshold at which an event such as a security breach or network outage renders a service unavailable, causes harm to customers or consumers, or poses a risk to market integrity.
- ☑ **Test resilience**. Once a cyber resilience program is in place, testing performance and assumptions under various scenarios assures objectives can be maintained.
- ☑ **Communicate disruptions**. Having a plan for clear, timely and relevant stakeholder communications (internal parties, partners, customers, regulating authorities) in the event of operational disruptions is essential for compliance, response, and recovery.

Acquiring Capabilities

Finally, it's important to determine what your organization needs to achieve its objectives, assess your current toolkit, and invest in new technologies to close the gap. Here are three capabilities you'll need to add for operational resilience.

- ☑ **Network Configuration Backup and Recovery:** by automating backup and recovery, organizations can respond faster and recover from failures or errors by restoring configurations (often in seconds) from a secure, centralized repository.
- ☑ **Change Detection and Compliance Auditing:** by automating change detection—including when, where, and who—and comparing against authorized settings, organizations can maintain compliance, close risk gaps, and eliminate lengthy manual audits.
- ☑ **Change Automation:** by automating bulk updates, whether in real-time or as a part of a scheduled maintenance and management program, human error is minimized, and time saved.

Automating these processes can reclaim as much as 40% of an IT team's time by eliminating repetitive, manual tasks, freeing them to focus on higher value tasks.

Skylar Compliance (formerly Restorepoint) and Skylar One (formerly SL1) can help achieve cyber resilience by modernizing and unifying your infrastructure tools, reducing complexity in day-to-day operations and automating workflows across your IT ecosystem for coordinated and efficient operations.

Gain end-to-end service visibility across complex hybrid environments to understand business impact

Leverage machine learning (ML) and AIOps analytics for proactive operations at scale

Benefit from configuration management, change automation and compliance auditing across your network estate

Automate workflows across your IT ecosystem for coordinated and efficient operations

Easily extend the platform to support your specific needs via low-code interfaces

Get up and running with minimal business impact with dedicated professional services.

Contact ScienceLogic to learn more and get a demo of Skylar Compliance and Skylar One.