ScienceLogic

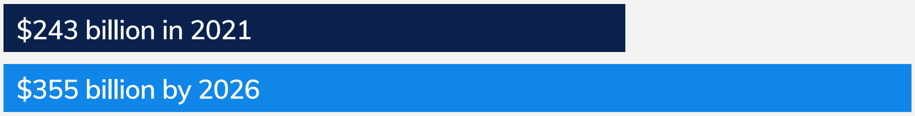
SOLUTION BRIEF

Network and Security Compliance for MSPs: What Leadership Needs to Know

Managed service provider (MSP) CEOs face recurring hurdles. In a survey by CRN, several MSP leaders pointed to four themes shaping their future success:

- Keeping existing technology running amid supply chain constraints
- Differentiation in a highly competitive market
- Maintaining strong security and cyber hygiene
- Hiring and retaining IT talent

These concerns are magnified in a rapidly growing MSP market--projected to expand from $243 billion in 2021 to nearly $355 billion by 2026 and expected to surpass $1 trillion by 2033. Successfully addressing them requires strengthening technical operations with a focus on resilience, reliability, and compliance. reliability, and compliance.



$112 billion

rapid growth forecasted in the MSP market by 2026

ScienceLogic's Skylar Compliance (formerly Restorepoint) a solution for network configuration backup, recovery, compliance analysis, and change management plays a crucial role for MSPs.

Here's how.

- Compliance Management Makes Business Sense
- Why Compliance Matters for MSPs
- Ensuring Reliable Compliance Management
- Four Best Practices for MSP Compliance
- Five Questions to Ask Before an Incident
- How Skylar Compliance Helps

Compliance Management Makes Business Sense

Cybersecurity isn't only about preventing cyberattacks and avoiding data breaches--it's also about complying with the many security and privacy regulations that govern how sensitive data is protected and managed. This includes financial, healthcare, personal, and intellectual property data. Compliance builds brand trust, and brand trust translates into a competitive edge.

Whether an MSP specializes in healthcare, retail, financial services, or another sector, it must meet a range of local, national, international, and industry regulations and standards to earn customer trust and avoid penalties for non-compliance.

Below are some key examples from across the globe:

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)

46%
of European managed service providers are concerned about security issues.

Why Compliance is Essential for MSPs

In May 2022, the U.S. Cybersecurity & Infrastructure Security Agency (CISA) and FBI, along with their "Five Eyes" counterparts in Australia, Canada, New Zealand, and the UK, issued a joint advisory highlighting threats specific to MSPs. The advisory recommended that customers contractually obligate MSP partners to demonstrate security compliance.

Certifications provide useful proof points, but the real measure is delivering consistently high-quality service. MSPs that fail to meet expectations risk losing business.

Today, executives are also on notice: they may be held personally liable for failing to meet compliance demands. In a precedent-setting 2023 case, a former Uber CISO was sentenced to three years' probation for failing to disclose a breach and for felony obstruction.

ISACA (Information Systems Audit and Control Association) recommends corporate management focus on six critical areas of compliance oversight:

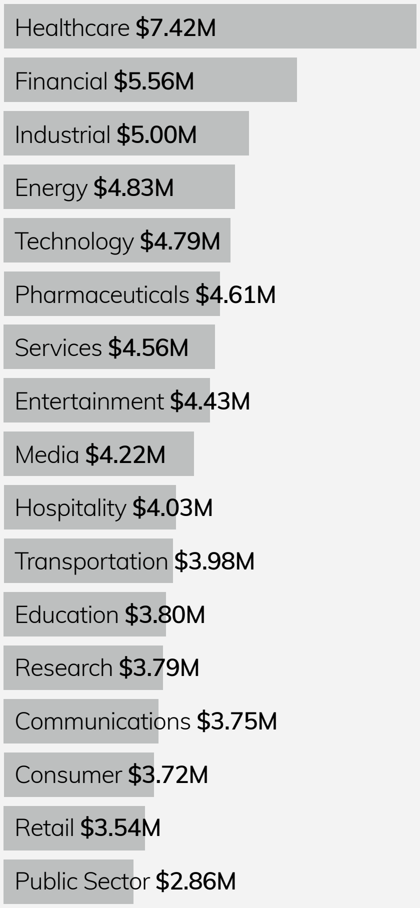
1. Employee awareness
2. Risk assessment
3. Patching
4. Compliance
5. Audits
6. Incident reporting

> "Cybersecurity oversight has now become the most important topic for the Board after strategic planning."
>
> **2021 Deloitte: The Changing Role of the Board on Cybersecurity: Robust oversight "Now" for a secure "Next"**

Common Technical and Professional Certifications & Standards

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Information Privacy Professional (CIPP)
- Certified Information Security Manager (CISM)
- ISO 27001
- Payment Card Industry Digital Security Standard (PCI-DSS)
- NIST Cybersecurity Framework
- System & Organization Controls 2 (SOC2)
- Network and Information Security Directive 2 (NIS2)

According to the 2025 Ponemon Institute/IBM Cost of a Data Breach Report, the global average cost of a data breach was $4.45 million per incident. Costs vary significantly by industry.



The Importance of Thorough and Reliable Compliance Management

For MSPs, maintaining security and compliance across both their own systems and their customers' environments can be complex and resource-intensive. Manual checks demand significant staff time and may leave gaps between audit cycles.

By automating compliance checks, Skylar Compliance can cut staff time devoted to these tasks by more than 50% and run checks daily as part of the backup process. This reduces the risk of misconfigurations or intrusions going undetected and strengthens overall security and reliability.

Four Compliance Best Practices for MSPs

To reduce the risk of data breaches and costly regulatory fines, MSPs should adopt these best practices:

1. **Centralize change management:** Actively track, verify, and manage system and configuration changes from a single point of control.
2. **Automate compliance checks:** Build and manage automated checks that strengthen security and demonstrate compliance to auditors and customers.
3. **Restore with confidence:** Implement a failsafe mechanism to automatically roll back configurations to compliant versions.
4. **Break down silos:** Eliminate operational silos when managing multiple network technologies and customer environments.

Skylar Compliance Can Help

The right tools make compliance fast, accurate, and fully documented. Automating repetitive processes such as audits and backups not only reduces risk and cost but also ensures consistent results.

Skylar Compliance automates key steps in network compliance and change management, saving MSPs up to **50% of staff time** and an average of **15,000 labor hours per year** — all while improving accuracy and reliability.

Contact ScienceLogic for more information.

Five Questions to Ask Before an Incident Occurs

To prepare and prioritize a Network and Security Compliance plan, ScienceLogic's Governance, Risk, and Compliance experts recommend leadership ask these five questions:

1. Is our network risk quantified and appropriately prioritized?
2. Is our backup strategy centralized, robust, and fit for purpose?
3. What are our current incident response times to outages or breaches?
4. How are we managing our compliance obligations?
5. What would it cost the business if an incident revealed gaps in meeting customers security or availability requirements?

| www.sciencelogic.com