SPOTLIGHT

Sponsored by: Cloudflare

Organizations continue to have low confidence in their security and compliance postures despite dedicating more resources to them. In this Spotlight, we show where security frameworks and compliance standards overlap and what organizations can do to strengthen their approaches to security and compliance.

Navigating Evolving Compliance Requirements with Streamlined Security Controls

January 2025

Written by: Grace Trinidad, PhD, Research Director, Trust Measurement and Metrics

Introduction

Across industries, regulatory compliance has become a thorn in the side. The number of organizational hours dedicated to compliance has risen as companies navigate expanding regulatory frameworks and increasing regulatory oversight. As part of this trend, organizations must contend with new frameworks without established guidance, global policies and regulations that require tailored regional approaches, cybersecurity, data privacy, and data sovereignty and localization concerns that continue to grow and complicate approaches to cybersecurity, in addition to the management of new technologies such as AI. Compliance is also increasingly public and very much a part of brand trust.

However, some organizations find that increasing the resource hours dedicated to compliance has not yielded greater confidence in their compliance posture. According to IDC's September 2023 *Worldwide Future of Trust Survey*, just 50% of the IT leaders and decision makers surveyed felt "completely prepared" to deal with regulatory compliance management while 42% felt "somewhat prepared" and 7% feel "somewhat unprepared" (see Figure 1).

AT A GLANCE

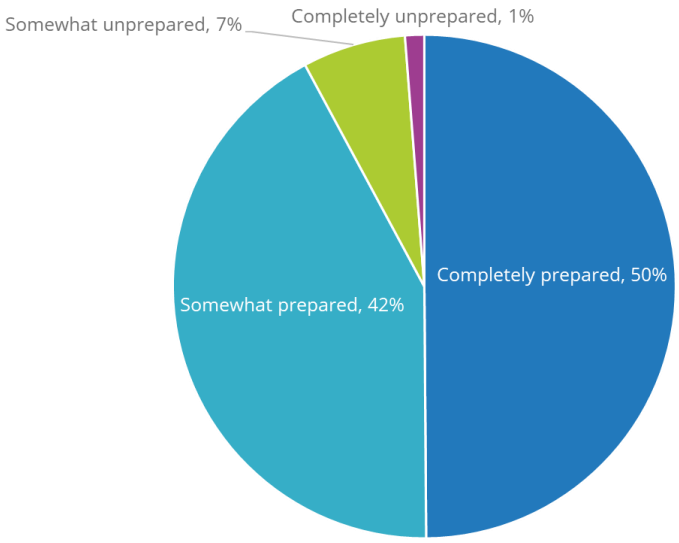
KEY STATS

Despite the resources dedicated to compliance management, organizations continue to doubt the strength of their compliance posture. According to IDC:

- 49% of organizations feel only somewhat prepared or somewhat unprepared to deal with regulatory compliance management.
- 35% of organizations report that "challenges in adopting/aligning AI governance to rapidly changing AI technologies" is the greatest barrier to AI adoption for their organization.
- 50% of organizations identify "data security and compliance" as the top infrastructure-related concern hampering their ability to move AI from proof of concept to production use.
- 32% of respondents worldwide state that "auditing for compliance" is the most important or second most important capability when evaluating AI platforms, indicating that organizations expect AI platforms to adhere to compliance frameworks.

FIGURE 1: ***Organizational Readiness for Regulatory Compliance***

Q How prepared is your organization to deal with regulatory compliance management?



Source: IDC's Worldwide Future of Trust Survey, September 2023

While every business seeks to be completely prepared in dealing with the management of regulatory compliance, policy, and data privacy, several forces work against a cohesive organizational approach to the problem. These include organizational silos, talent and resource shortages, rapidly changing regulations worldwide, and lack of continuous monitoring. In detail:

- **Organizational silos:** Silos, department divisions, and poor interdepartmental communication can result in disjointed approaches to regulations and gaps in how they are addressed. Close collaboration between security, privacy, and compliance functions — at minimum — is necessary to address regulatory compliance in a holistic manner.
- **Talent and resource shortages:** Cybersecurity talent shortages plague organizations worldwide. This challenge is exacerbated by both the complex threat landscape and the increasing involvement of cybersecurity leadership in all areas of an organization, including compliance.
- **Rapidly changing regulations worldwide:** If only regulations and laws were issued around the same time and were accompanied with clear compliance guidance. Until such miracles occur, industries have to navigate existing and proposed regulations dynamically, resulting in low confidence that compliance posture is robust. Some organizations are turning to the more stringent guidelines put forth by the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC).

- **Lack of continuous monitoring:** In *IDC FutureScape: Worldwide Future of Trust 2024 Predictions* (IDC #US51293523, October 2023), IDC analysts predicted that "by 2026, 40% of organizations will utilize AI-enabled risk and compliance solutions to continuously monitor data in real time and to predict noncompliance internally or from third-party associations." Without continuous monitoring, weaknesses in an organization's compliance posture may go unnoticed until a major violation occurs.

Strategies for Managing Evolving Compliance Regulations

Organizations that seek to minimize the time and effort needed to maintain regulatory compliance have several strategies to consider, including:

- **Prioritizing critical risks for more efficient security resource allocation:** As digital infrastructures become more complex, the risks introduced into organizational environments by this complexity have overwhelmed CISOs and their teams. It is, therefore, necessary to identify as many risks to the organization as possible — not a small effort but a critical one. Those risks can then be triaged to provide cybersecurity and compliance teams with strategic guidance to determine where they should prioritize their efforts.
- **Reengineering business functions for a more holistic approach to incorporating necessary compliance efforts:** Internal reorganization for holistic security and compliance management is related to the prioritization of critical risks because culture change can be difficult. Security and compliance cohesion can be a starting point for broader change across the organization.
- **Reviewing existing security controls for alignment with compliance frameworks:** This document highlights where frameworks align with security controls. It can be used to review where controls support regulatory compliance and where gaps may remain.
- **Streamlining compliance by using the platform approach:** Trust platforms, trust centers, and other security and compliance functions are offered by several cloud-based vendors. Many leverage their own internally collected high-quality data to improve the security and compliance posture of their customers, continuously updating their platforms and educating their customers as new compliance considerations arise.
- **Employing compliance automation:** Compliance automation leverages AI and other technologies to provide real-time information on an organization's compliance posture. Not all vendors offer compliance automation yet, but it will become standard in time as AI adoption grows and the number and scope of regulatory requirements increase.

Each of these strategies is valuable but bringing them together compounds their power. By leveraging a comprehensive risk management strategy, unified policies, and modular platforms that provide compliance automation, businesses can create a future-ready compliance framework that aligns with global standards while maintaining operational flexibility and resilience.

The ability to set security policies once and propagate them across all environments ensures consistency and reduces the risk of errors, creating a seamless foundation for compliance management. A modular platform approach allows organizations to adapt to specific needs, such as data sovereignty or regional regulations, while integrating new technologies and processes. This scalability is critical as compliance standards evolve alongside the dynamic threat landscape.

Moreover, modular security platforms that support cross-industry and cross-regulation compliance empower businesses to address overlapping security frameworks, streamline audits, and ensure a robust posture in diverse regulatory contexts, including cloud environments. The number of security frameworks and compliance standards in play can cause concern that organizations have coverage gaps — but a closer look shows a significant overlap between many of them.

Cybersecurity Controls and Compliance Standards Overlap

Implementation of cybersecurity controls to meet compliance obligations can be challenging. In addition to the challenges of compliance, organizations are up against a chronic cybersecurity talent shortage, regulations that continue to evolve, and new and revised offerings from vendors. Taken together, it's easy to see why confidence in compliance posture is low. AI and generative AI (GenAI) compound this uncertainty, as all organizations anticipate new regulations to assuage concerns about the trustworthiness of these technologies. As cited in *How Important Is Auditability for Compliance in Selecting a GenAI Platform* (IDC #US52343024, June 2024), 32% of all respondents worldwide stated that "auditing for compliance" was either the most important or second most important capability when evaluating AI platforms, thus indicating a desire for AI platforms that are explicit in their alignment with regulatory and compliance frameworks.

An Overview of Key Compliance Standards and Selected Security Controls

Table 1 shows a selection of security frameworks and compliance standards that many organizations must adhere to. Where available, the table indicates where guidance pertaining to the selected security control can be found in that document (e.g., IA-2, Article 9). Controls are otherwise marked with an "X" when a reference or citation is not available in the corresponding framework.

TABLE 1: *Overview of Key Compliance Standards and Selected Security Controls*

	Selected Security Controls										
Key Compliance Standards	Asset and Config. Mgmt	Identity and Access Mgmt (IAM)	Data Protection and Encryption	Network and Comms Security	Endpoint and Device Security	System and Application Security	Logging and Monitoring	Incident Response (IR) and Business Continuity	Data Localization	Physical Security	Awareness and Training
NIST 800-53 — Security and privacy controls for information systems and organizations*	CM-1 – CM-14	AC-2 AC-6 IA-2 – IA-4	SC-12 SC-13 MP-5	SC-7; SC-13 AC-17	CM-7 CM-8 SI-3	SA-11 SI-2 SI-10	AU-2 AU-6 AU-12	IR-4 CP-2	SC-4 MP-5	PE-3 PE-6 PE-12	AT-2 AT-3
NIST 800-171 — Protecting unclassified information in nonfederal systems and organizations	CM-1 – CM-12	AC-2 AC-6 IA-2 – IA-4	SC-12 SC-13	SC-7 SC-8	SI-3 SI-4	SI-2 SI-10	AU-2 AU-6	IR-4 CP-2		PE-2 PE-3	AT-2 AT-3
NIST 800-207 — Zero trust architecture	X	X	X		X	X	X	X			X
ISO 27001 — Security management system*	A.5.9 A.5.10 A.8.9	A.8.1 A.8.3 A.8.4	A.8.11 A.8.24	A.8.23	A.8.10	A.8.10 A.8.28	A.8.15 A.8.16	A.5.25 A.5.30	A.5.29	A.7.1 A.7.2 A.7.4	A.6.2 A..6.3
ISO 27018 — Protection of personally identifiable information	X	X	X	X	X	X	X	X	X	X	X
CIS*	C1 C2 C4	C5 C6	C3 C11	C9 C12	C1 C7 C10	C8 C16	C8 C12	C11 C17	C3	C1	C14
Federal Risk and Authorization Management Program (FedRAMP) – Adopts but modifies NIST 800-53	X	X	X	X	X	X	X	X		X	X
AICPA SOC 2 Type II/ TSC*	CC5.2 CC5.4 CC6.1	CC5.4 CC6.2 CC6.3	CC6.6 C1.1	CC6.7 CC6.8	CC6.4 CC6.5	CC7.1 CC7.2	CC7.2 CC7.3 CC7.4	CC7.1 CC7.4 CC7.5 CC9.2	CC1.2	CC6.1 CC6.2	CC3.2 CC3.3
DORA	Article 8	Article 9	Article 9	Article 9	Article 9	Article 9	Article 10	Article 11	Article 30	Article 9	Article 13

	Selected Security Controls										
Key Compliance Standards	Asset and Config. Mgmt	Identity and Access Mgmt (IAM)	Data Protection and Encryption	Network and Comms Security	Endpoint and Device Security	System and Application Security	Logging and Monitoring	Incident Response (IR) and Business Continuity	Data Localization	Physical Security	Awareness and Training
TIC 3.0 — Trusted Internet Connections	X	X				X	X	X			
Payment Card Industry Data Security Standard (PCI DSS)	Reqmt 2.4	Reqmt 7 Reqmt 8	Reqmt 3 Reqmt 4	Reqmt 1 Reqmt 2	Reqmt 5	Reqmt 6	Reqmt 10	Reqmt 12		Reqmt 9	Reqmt 12.6
Sarbanes-Oxley Act (SOX)	X	X	X	X	X	X	X	X		X	X
Cybersecurity Maturity Model Certification (CMMC)*	CM L2; CM L3	AC L1, L2, L3 IA L1, L2, L3	MP L1, L2 SC L2	SC L1, L2,L3	SI L1, L2, L3	CA L2, L3 SI L2, L3	AU L2	IR L2, L3 RA L2, L3 SI L1, L2 CP L2	SC L2, L3	PE L1, L2	AT L2, L3
Health Insurance Portability and Accountability Act (HIPAA)	X	X	X	X	X	X	X	X		X	X
Cloud Computing Compliance Criteria Catalogue (C5)	5.6	5.7	5.8	5.9	5.10	5.10	5.11	5.12	4.1	5.14	5.15
High C — Part of the confidentiality, integrity, and availability (CIA) triad	X	X	X	X	X	X	X	X	X	X	X
General Data Protection Regulation (GDPR)		X	X	X		X	X	X	X	X	X
EU AI Act	17	15(5)	10 15(5)	15(5)	15(4)	15(4)	19	9			17
NIS2 Directive*	21(2)(a)	21(2)(d)	21(2)(e)	21(2)(b)	21(2)(c)	21(2)(a)	21(12)(f)	21(12)(b) 21(12)(c)	21(12)(e)	21(2)(g)	20(2)

** The standard is comprehensive in its coverage.*

Note: NIST 800-53 is a comprehensive document that provides greater depth on the relationships between controls. For example, within NIST SP 800-53, Rev. 5, the authors indicate that IA-2 (Identification and Authentication) is closely related to AC-2, AC-3, AC-4, MA-4, MA-5, PE-2, and SA-8, among other controls.

Source: IDC, 2025

While Table 1 highlights the overlap between key compliance standards and selected security controls, an in-depth look at the various controls follows. Within each broad category of security controls are subcategories that illuminate why alignment of controls with regulatory frameworks can be overwhelming. Organizations must determine which of the 11 subcategories in the following sections (as previously listed in Table 1) best match the needs of their own environments.

Asset and Configuration Management

Present across most of the regulatory controls mentioned in Table 1, asset and configuration management provides the visibility, control, and structure necessary to holistically protect an organization's systems and data. Asset management establishes a clear understanding of what assets exist and the protections required to properly secure them. Configuration management defines and enforces secure settings based on asset type. Improper configurations are responsible for many security breaches, but proper configuration depends on first correctly identifying and managing organizational assets.

Asset and configuration management includes asset inventory, an up-to-date inventory of all physical and digital assets in a centralized, visible, and reportable manner, classified based on sensitivity and criticality; configuration management, which is the maintenance of secure configuration baselines for systems and devices; and supply chain security and supply chain management, which encompasses all process and entities involved in producing and delivering services. Supply chain security focuses on mitigating risks that can arise from third-party vendors, suppliers, and service providers such as data breaches, operational disruptions, and cyberattacks exploiting vulnerabilities in external systems. Recent attacks on companies such as SolarWinds and Kaseya underscore the importance of supply chain security and management.

Identity and Access Management

Access controls and identity management (alongside system and application security) is the foundation of security and is present across every regulatory framework and standard. These controls govern how users, devices, and systems interact with organizational resources and require close and continuous management. This area has five key offerings: identity management defined as the creation, management, and authentication of digital identities for users, devices, and systems; access management, which is the definition and enforcement of access permissions based on roles, responsibilities, and risk levels (role-based access controls); least privilege; multifactor authentication (MFA); and identity verification. Zero trust architecture is an increasingly used approach to IAM whereby trust is never assumed and must be continuously verified at every access attempt based on identity, resource, and device health.

Data Protection and Encryption

Data protection and encryption is a critical component of security and is present across most of the frameworks and standards mentioned in this paper. It mitigates security risks and aligns with mandated stringent measures to safeguard personal and financial information.

Data protection encompasses a range of practices designed to secure information throughout the data life cycle. This includes robust access controls, data classification, and data governance policies to ensure that only necessary information is collected, processed, and stored. Encryption, a cornerstone of data protection, ensures that sensitive data is rendered unreadable to unauthorized users. By encrypting data at rest and in transit using strong cryptographic algorithms (e.g., AES-256 and transport layer security [TLS] 1.2+), organizations protect against data breaches and man-in-the-middle attacks. Even if attackers access encrypted data, it remains unusable without the appropriate decryption

keys. For developers, data masking and anonymization enable the protection of sensitive data used in development and testing environments. Data masking and anonymization is, therefore, a key component in developing and testing technologies such as AI.

Network and Communications Security

Network and communications security is critical for ensuring the confidentiality, integrity, and availability of information transmitted across an organization's infrastructure. As the backbone of digital operations, networks connect users, systems, and data. This makes them a primary target for cyberattacks, interception, or unauthorized access. Technologies such as firewalls, intrusion detection and prevention systems (IDS/IPS), and network segmentation reduce the attack surface and limit lateral movement, preventing attackers from compromising critical assets. However, this has become more complicated with the rise of remote work and flex work. As a result, organizations have increasingly turned to encrypted communications using TLS, VPNs, and IPsec to protect data in transit, ensuring it cannot be intercepted or tampered with during transmission.

Although present in most of the frameworks in Table 1, PCI DSS, GDPR, and HIPAA mandate stringent network security measures to protect sensitive data from modern threats, including ransomware, phishing, and distributed denial of service (DDoS) attacks. These risks further highlight the need for continuous network monitoring and anomaly detection. Approaches to securing networks and communications include network segmentation in which networks are segmented to isolate sensitive systems and mitigate lateral movement; zero trust architecture; and domain name system (DNS) security, which implements DNS filtering and DNS security extensions to prevent spoofing and phishing.

Endpoint and Device Security

Critical to the regulations and frameworks in Table 1 is ensuring that organizations protect devices handling sensitive information. This requirement becomes more complex to enforce when key personnel with access to sensitive information work from home or other remote locations. Endpoints such as laptops, smartphones, tablets, and Internet of Things (IoT) devices can act as gateways to an organization's sensitive data and networks. Endpoint vulnerabilities can be and are often shared with the entire network. Tools such as endpoint detection and response (EDR), antimalware solutions, and mobile device management (MDM) help mitigate the risks that endpoints pose by detecting, preventing, and responding to potential threats in real time. When used with data protections and encryption, access controls, and patch management, these tools can ensure an organization's devices meet the required security standards. Endpoint security tools also facilitate compliance by providing audit logs and monitoring capabilities, which are essential for demonstrating adherence during audits.

System and Application Security

System and application security is the core of cybersecurity practices and is required for every framework in Table 1. Vulnerabilities in systems and applications such as unpatched software, misconfigurations, or weak coding practices can lead to data breaches, service disruptions, or unauthorized access. Secure system configurations, vulnerability management, and secure software development life-cycle (SDLC) practices are essential for reducing these risks. Implementing measures such as penetration testing, code reviews, and runtime application self-protection ensure that security is integrated into every stage of application development and deployment.

In addition, the proliferation of APIs necessitates robust API security measures, employing tools such as API gateways, rate limiting, and authentication standards such as OAuth 2.0 and OpenID Connect to thwart attacks. Cloud-native

environments require expertise and management in container security, Kubernetes security, and infrastructure as code (IaC) scanning to mitigate risks such as misconfigurations and privilege escalation. Advanced technologies such as AI and machine learning (ML) are increasingly used to enhance security, enabling predictive threat detection, behavioral analysis, and real-time response automation. EDR and extended detection and response (XDR) systems further streamline threat visibility across endpoints and networks, aligning with the trend toward unified security management. Furthermore, the rise of DevSecOps accelerates the shift-left approach, embedding security into CI/CD pipelines and enabling developers to address vulnerabilities earlier in the development cycle.

Logging and Monitoring

Critical to every regulation and framework, logging and monitoring are the backbone of organizational audit and reporting. Logging captures detailed records of activities within an organization's systems, applications, and networks, supporting regulatory requirements for accountability and transparency. These logs include user access, system changes, and network activity, offering a comprehensive view of operations. When security events occur, logs help identify the root cause, the scope of impact, and the perpetrators. This insight enables organizations to refine defenses and prevent future incidents. Monitoring adds an active layer by analyzing logs and system behaviors in real time. Tools such as security information and event management (SIEM) systems and IDS/IPS detect anomalies, flag unauthorized activities, and trigger alerts. Early detection of threats, such as brute-force attacks or malware infections, allows for immediate response, thus reducing potential damage. AI and ML have expanded on monitoring capabilities, providing predictive analytics to identify threats proactively and discern subtle environmental deviations that can indicate external or internal threats.

Without robust logging and monitoring, organizations face blind spots that attackers can exploit, increasing the risk of undetected breaches. By implementing comprehensive logging and continuous monitoring, organizations enhance their ability to protect sensitive data, maintain operational integrity, and meet compliance obligations.

Incident Response and Business Continuity

Incident response is relevant to all the frameworks in Table 1. It involves structured processes to detect, contain, eradicate, and recover from security events such as data breaches, ransomware attacks, or insider threats. A well-defined IR plan enables organizations to act quickly, reducing damage and preventing escalation. It also facilitates post-incident analysis, allowing teams to identify vulnerabilities and improve defenses. IR plans include defined roles, comprehensive playbooks, and regular drills to ensure readiness. Integration of advanced tools such as security orchestration, automation, and response (SOAR) platforms and AI-driven threat detection systems has improved response speed and accuracy, making real-time mitigation achievable. Collaboration with external stakeholders such as incident response teams, government entities, and third-party vendors also enhances preparedness. Business continuity complements IR by focusing on maintaining or quickly restoring critical business operations during disruptions. It ensures that the organization can maintain or quickly restore essential functions during and after an incident. Business continuity plans address risks such as prolonged outages, data loss, and operational disruptions, which can have severe financial, reputational, and legal consequences. By incorporating disaster recovery strategies and regular testing, organizations can ensure resilience against unexpected events, such as cyberattacks or natural disasters. This involves creating and testing business continuity and disaster recovery plans to address risks. A key evolution in business continuity is the adoption of cloud-based solutions for redundancy, enabling organizations to shift operations swiftly to alternate environments.

Recent advances emphasize the convergence of cybersecurity and business continuity practices, driven by trends such as hybrid work models, ransomware sophistication, and supply chain attacks. Zero trust architecture is becoming integral to both IR and continuity strategies, ensuring minimal exposure even during breaches. In addition, tabletop exercises incorporating scenario-based simulations help teams practice coordinated responses and adapt plans based on lessons learned. Cybersecurity insurance, though increasingly costly, is another component of modern business continuity planning, providing financial coverage for recovery and reputational damage.

Data Localization

Data localization and digital sovereignty mandates require organizations to store, process, or handle specific data within the geographic boundaries of a country. These mandates are influencing global cybersecurity and compliance landscapes. As part of digital sovereignty efforts, governments worldwide are implementing data localization laws to bolster national security, protect citizens' privacy, and ensure regulatory oversight. Key examples include GDPR, which restricts data transfers to noncompliant regions; China's Cybersecurity Law mandating in-country storage of certain data; and India's proposed data protection frameworks. Other nations, such as Russia, Indonesia, and Brazil, have introduced sector-specific or broad mandates impacting financial, health, and government data.

Localization affects datacenter strategies, often necessitating partnerships with local cloud providers or building in-country infrastructure, both of which carry cost and complexity implications. Data localization demands robust mechanisms to segregate, encrypt, and monitor data across jurisdictions while ensuring accessibility and uptime. However, data localization also introduces cybersecurity challenges. Localizing sensitive data increases exposure to localized threats, including state-sponsored actors or insufficiently secure infrastructure in emerging markets. Compliance with data localization mandates often necessitates stringent data transfer protocols and security frameworks such as encryption, tokenization, and zero trust architectures. Regular audits and real-time monitoring of cross-border data flows become vital to minimize risks. Emerging technologies such as privacy-enhancing computation and secure multiparty computation hold promise in facilitating compliant data sharing.

Data localization efforts must also be embedded into enterprisewide data governance policies. This includes classifying data by sensitivity and jurisdiction, conducting impact assessments, and ensuring compliance through automated tools. Educating stakeholders on the financial, legal, and operational implications of noncompliance is equally critical.

Physical Security

Physical security is a critical component of a comprehensive security and compliance strategy and ensures that facilities, hardware, and the devices holding organizational assets are secure from unauthorized access, tampering, and theft. Modern physical security encompasses traditional measures such as access control systems, surveillance cameras, and security personnel but has evolved with advancements in technology. Biometric authentication (e.g., facial recognition and fingerprint scanners) and AI-driven surveillance systems provide enhanced accuracy and reduced manual monitoring overhead. IoT-enabled devices, such as smart locks and sensors, enable real-time monitoring and response, integrating seamlessly with cybersecurity frameworks to detect and prevent both physical threats and cyberthreats. However, these innovations bring their own vulnerabilities. As previously mentioned, IoT devices can be a gateway to an organization's network, making them an attractive target for cyberattacks.

Awareness and Training

Cyberattackers have historically used and will continue to use phishing, social engineering, and ransomware to infiltrate systems, exploiting human behavior to access key resources. The prospect of human error means the majority of regulations require organizations to implement security awareness and training initiatives. These programs ensure that employees understand their responsibilities for protecting sensitive data, adhering to access controls, and reporting potential security incidents. Role-based training for employees handling high-risk information further enhances compliance by addressing specific regulatory requirements.

Benefits

Once a strategy for securing an organization has been selected, many companies move to modular, platform-based approaches to security, compliance, and data protection. These platforms allow organizations of all sizes to capitalize on a provider's expertise and large data sets to drive more responsive and up-to-date maintenance of security and compliance. By leveraging these advanced tools and practices, businesses can achieve compliance across diverse frameworks, industries, and geographies while maintaining flexibility and control.

A platform-based approach to security and compliance allows organizations to establish policies once and propagate them seamlessly across their entire environment. By harmonizing business functions and centralizing compliance settings and controls, businesses can enforce consistent security and data protection standards across applications, systems, and cloud environments. This reduces the risk of policy drift and ensures uniform adherence to regulatory requirements. Automated policy proliferation streamlines operations, minimizes manual errors, and enables rapid adjustments to evolving regulations.

Organizations need systems that can accommodate new requirements without overhauling existing frameworks. A platform approach to compliance can offer tools that anticipate emerging trends in data governance and regulatory overlap. Features such as built-in automation, machine learning for threat detection, and centralized dashboards enable organizations to monitor compliance metrics in real time, ensuring readiness for new laws and standards.

Considering Cloudflare

Headquartered in San Francisco, Cloudflare operates a global network that spans over 300 cities in more than 100 countries, enabling rapid content delivery and advanced threat mitigation. The company's key focus areas include website performance optimization, DDoS protection, and zero trust security. Cloudflare's extensive edge network provides robust capabilities for mitigating cyberattacks at scale while maintaining low latency. One cornerstone offering is the DDoS protection service designed to prevent large-scale attacks that aim to overwhelm online resources. The company's network capacity exceeds 100Tbps, enabling it to neutralize massive DDoS attacks. This service is complemented by the web application firewall (WAF), which uses machine learning to identify and block malicious traffic while allowing legitimate traffic to pass through. The WAF is updated continuously with global threat intelligence, offering strong protection against SQL injections, cross-site scripting (XSS), and other application-layer attacks.

In recent years, Cloudflare has expanded its portfolio to address the shift toward zero trust security architectures. Cloudflare's SASE platform enables secure access to internal applications and corporate data without relying on traditional VPNs, which are increasingly viewed as vulnerable to modern cyberattacks. The solution incorporates identity-based authentication and device posture verification, ensuring granular access control. Cloudflare's Magic Transit protects entire network infrastructures by routing traffic through Cloudflare's global network. This solution mitigates

volumetric DDoS attacks and provides improved network performance. In addition, Cloudflare offers solutions such as bot management, which uses behavioral analysis to distinguish between legitimate users and malicious bots, and email security, which safeguards against phishing and email-based attacks.

Challenges

While Cloudflare is a leader in DDoS protection and edge network performance, the company operates in a competitive and crowded market that has become increasingly difficult for customers to navigate. Customer organizations, such as cybersecurity companies themselves, are facing a continual cybersecurity and compliance talent shortage. This increases the demand for comprehensive, easy-to-understand offerings that are in alignment with key regulatory and compliance frameworks to help maintain confidence in an organization's own security and compliance posture. Furthermore, Cloudflare and its marketplace peers are increasingly expected to stay in front of and anticipate regulatory compliance needs and offer updated and new technologies to meet these changes.

In IDC research evaluating the compliance priorities of IT buyers and decision makers, North American respondents ranked "compliance certifications with global, national, and industry standards" as the most important area of compliance in 2024 (see *Compliance Certifications Lead Compliance and Trust Ranking for 2024,* IDC #US52776424, December 2024). This differs from previous years where "skilled staff and leadership in global regulatory compliance" and "trust centers or information and guidance on security, privacy, and compliance adherence" were the most important areas, signaling the changing priorities of customer organizations. Cloudflare, like other companies in this space, must reorganize its offerings to align with this desire for compliance certifications.

Conclusion

As organizations navigate an increasingly complex regulatory environment, face evolving cyberthreats, and leverage new cloud technologies such as AI, the importance of a holistic and solutions-based approach to security and compliance cannot be overstated.

Ultimately, adopting a comprehensive compliance strategy ensures that organizations are not only meeting their current obligations but also building resilience against future challenges. This approach fosters trust among stakeholders, safeguards sensitive data, and enhances operational efficiency, allowing organizations to thrive in a rapidly changing digital world.

The importance of a holistic and solutions-based approach to security and compliance cannot be overstated.

About the Analyst

Grace Trinidad, PhD, *Research Director, Trust Measurement and Metrics*

Grace Trinidad is research director in IDC's Security and Trust research practice responsible for the Future of Trust research program. In this role she provides strategic guidance and research support on approaches to trust that include risk, security, compliance, privacy, ethics, and social responsibility.

MESSAGE FROM THE SPONSOR

A new approach to security is needed for compliance in the digital world.

The convergence of tech (AI, APIs, cloud), global data sharing, and evolving regulatory frameworks presents challenges in striving to protect sensitive information while addressing compliance. Organizations' current approach is not working, resulting in:

- **Unnecessary costs:** Multiple siloed tools for security, sovereignty, and privacy
- **Inefficiency:** Manual processes for log collection and audit across disparate toolsets reduce productivity
- **Degraded performance:** Resulting from data localization constraints

To address regulations, organizations need a comprehensive strategy that takes into account data localization, security, and compliance. Compliance strategy should align with business objectives while also addressing evolving threats and security in the cloud including getting visibility into data, protecting and localizing data to meet data access, transfer, AI/application obligations, ensuring governance posture aligned to organization's risk profile and meeting audit and reporting requirements for internal and third-party audits.

Click here to learn how Cloudflare can help address compliance.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
blogs.idc.com
www.idc.com