Prepared for

CLOUDFLARE

The State of Data Security and Regulatory Compliance

August 2024 EMA White Paper

By **Christopher M. Steffen, CISSP, CISA**, VP of Research
Information Security, Risk, and Compliance Management

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

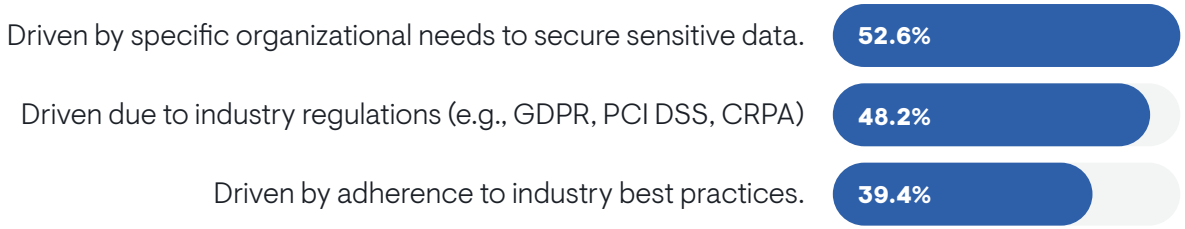
Introduction

Data security and regulatory compliance considerations are top of mind for nearly every technology executive. Industries of every size and in every vertical are forced to address these requirements. Sophistication of the data environment and strict regulatory necessities that govern organizations' operational environment necessitate strong compliance measures. As we gain better understanding of these considerations, technology leaders can prioritize these considerations and develop plans to address them in their organizations.

Recently, Cloudflare teamed with Enterprise Management Associates (EMA) to conduct a survey to investigate trends in data security and regulatory compliance. The survey looked at the drivers behind data security, the impacts on organizational performance, the location of various data stores, the use of specialized compliance solutions, and bandwidth organizations have to address these requirements.

Securing Sensitive Data Driving Data Compliance

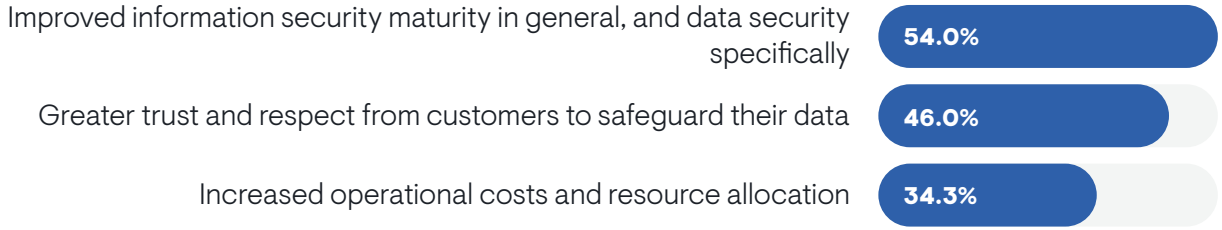
WHICH BEST DESCRIBES WHAT HAS DRIVEN YOUR ORGANIZATION'S JOURNEY IN DATA COMPLIANCE?



When EMA asked organizations how their journey toward data compliance began, 52.6% of respondents cited specific organizational needs to secure sensitive data. This underscores the importance of protecting critical information to prevent breaches and safeguard assets due to the increased threat landscape from the adoption of hybrid cloud, increases in AI attacks and modern app development processes. Additionally, industry regulations, such as GDPR, PCI DSS, and CRPA, drive compliance for 48.2% of organizations, highlighting the influence of regulatory frameworks in shaping data security strategies. Adherence to industry best practices drives an additional 39.4% of organizations, reflecting a commitment to maintaining high standards in data management and security.

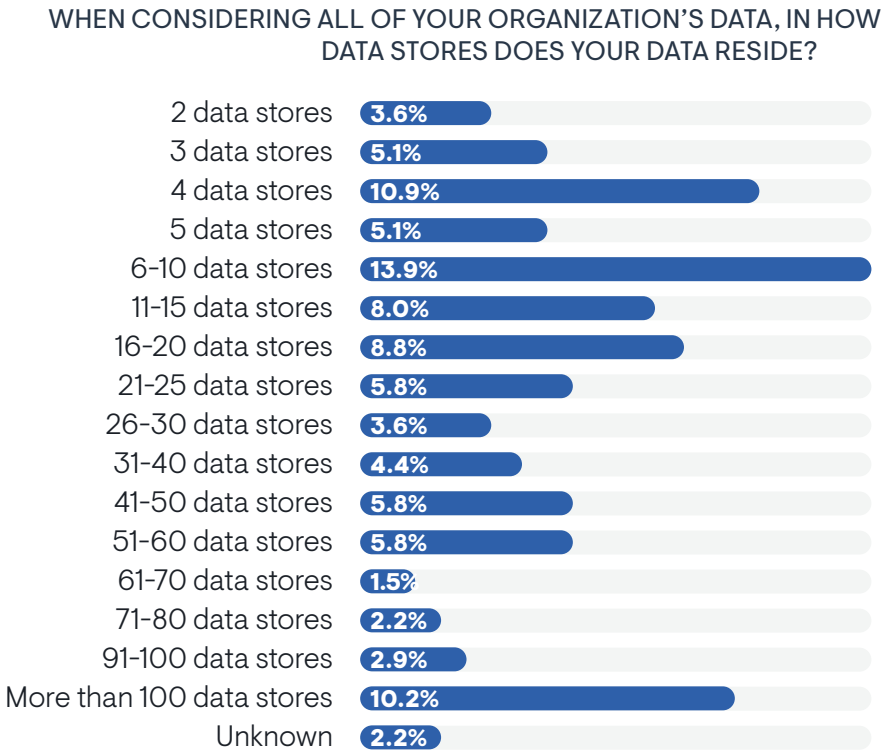
Compliance Enhances Security Frameworks Resulting in Organizational Performance and Growth

WHICH BEST DESCRIBES HOW YOUR ORGANIZATION'S DATA COMPLIANCE JOURNEY HAS IMPACTED YOUR ORGANIZATION'S INNOVATION/GROWTH/PERFORMANCE?



When asked about how their organization's data compliance journey impacted their organization's innovation/growth/performance, 54% of respondents report improved information security maturity, particularly in data security. This indicates that compliance efforts enhance overall security frameworks. Additionally, 46% of organizations indicate that data compliance fosters greater trust and respect from customers, enhancing reputational standing and customer loyalty. Thirty-four percent of organizations acknowledge that compliance leads to increased operational costs and resource allocation, reflecting the financial and logistical investments required to maintain compliance.

Data Dispersion and Management Increases Data Security Complexity

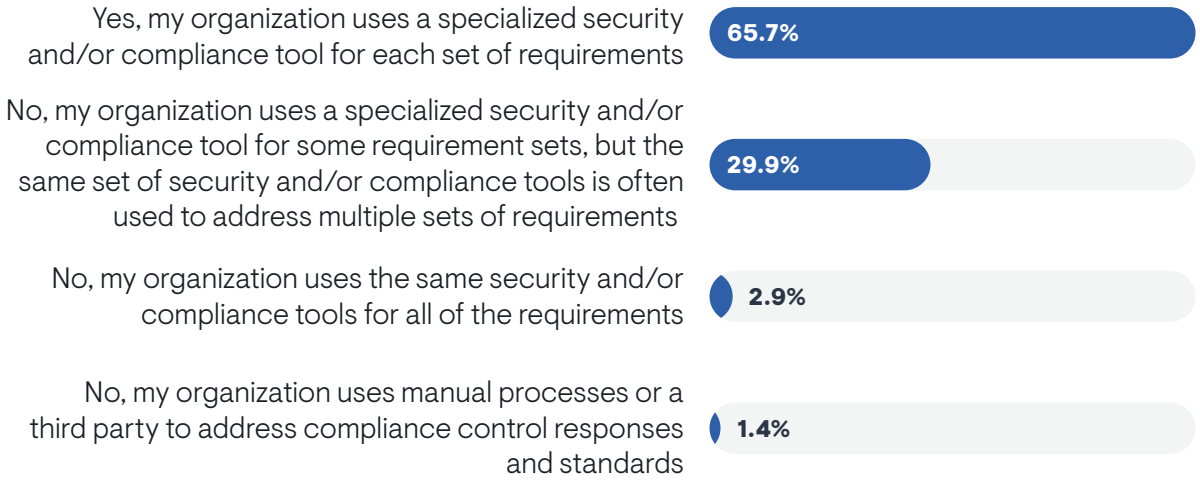


32.8% indicated that their data resided on 40 or more separate locations.

When asked about how many separate data stores organizations use, 32.8% of organizations said their data resides in 40 or more separate locations. Over 10% indicated that their organization had more than 100 data stores. This fragmentation is often a result of the growing adoption of cloud services and SaaS apps and the need for geographically distributed data storage. Managing data across numerous locations introduces significant challenges in ensuring data security and regulatory compliance. Each data store may have different security protocols, access controls, and compliance requirements, complicating the task of maintaining a uniform security posture.

Specialized Compliance Tools

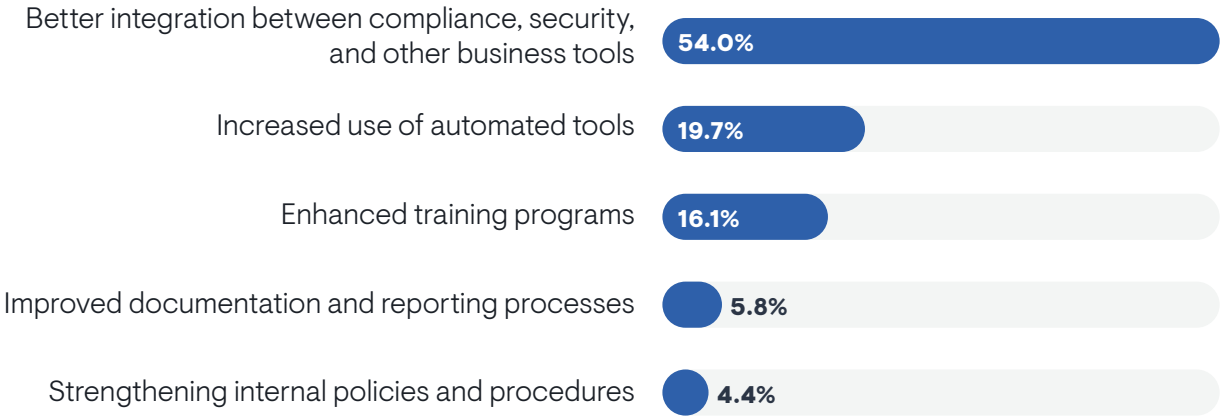
FOR EACH REGULATORY COMPLIANCE STANDARD/CONTROL SET THAT YOUR ORGANIZATION MUST COMPLY WITH, DOES YOUR ORGANIZATION USE A DIFFERENT SECURITY AND/OR COMPLIANCE TOOL TO HELP ADDRESS THE REQUIREMENTS?



The use of specialized tools to address different compliance requirements is prevalent among organizations. When asked, almost 66% of organizations said they use a specialized tool for each set of compliance requirements. This widespread adoption indicates that organizations recognize the importance of specific solutions to meet the diverse and stringent demands of various regulatory frameworks. However, the reliance on multiple specialized tools also introduces challenges, particularly in terms of integration and resource allocation.

Need for Better Integration

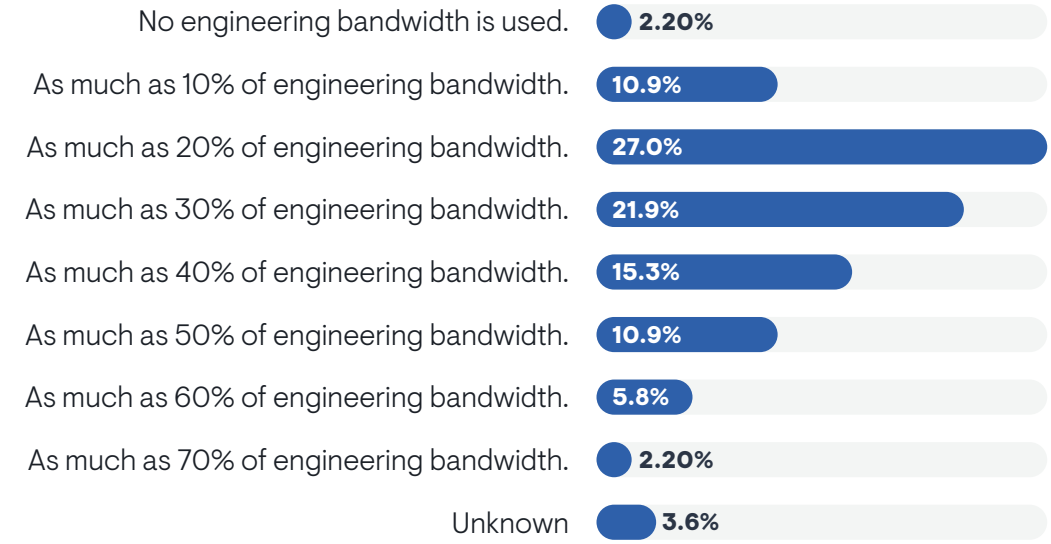
WHAT IS THE MOST IMPORTANT IMPROVEMENT YOU WOULD MAKE TO MEETING COMPLIANCE REQUIREMENTS/YOUR CORPORATE COMPLIANCE STRATEGY?



When asked about the most important improvement organizations would make to address compliance requirements, 54% indicated that they would look for better integrations between compliance tools and the solutions used for business processes. However, the improvement of the integration level can be troublesome, especially in organizations with a diversified IT environment.

Considerable Engineering Bandwidth Allocated to Compliance

WHAT PERCENT OF ENGINEERING BANDWIDTH DO YOU USE ON COMPLIANCE AUDITS?



Compliance audits require substantial resources from the organization. In this survey, 84% of the organizations indicated that they are allocating 20% or more of their engineering resources to compliance-related activities. This represents a significant commitment of vital organizational resources and reflects the complexity of modern compliance requirements. Compliance audits are critical for verifying adherence to standards such as GDPR, PCI DSS, and other regulatory frameworks, but they also consume a considerable portion of engineering time and resources.

Analysis and Conclusion

When looking at the results from the survey, three data points jump out as the most significant:

- **The need to secure sensitive data.** Few (if any) companies take on compliance-related controls without reason. The majority of organizations are trying to protect sensitive data, because of regulatory or vendor due diligence controls and due to the convergence of hybrid cloud, Gen AI, and global data sharing it is even more imperative to protect their organization's most valuable asset. Organizations also realize that as they address changing environments and evolving threats, protecting sensitive data becomes more of a challenge, but also a greater priority. There are plenty of quality solutions on the market (such as Cloudflare) specifically designed to help organizations with this goal. It is incumbent on organizations to find the budget and resources to enable a strong data security policy to deal with the variety of data-related controls they face.
- **Data, data everywhere.** It is extremely difficult to enact a data security plan. Every time someone discovers a new data source or data location, the plan multiplies in difficulty. Almost one-third of those surveyed indicated that they had 40 or more different data locations or stores (and those are the ones they know about). Ten percent indicated that they had over 100 different data stores. When considering data compliance issues, data geolocation concerns, and data governance, having such a wide and disparate array of data storage makes the job of securing that data extremely difficult. It would be impossible to accomplish without a data security and compliance solution to assist with the process.
- **The valuable resource cost of data compliance.** Possibly the most shocking data point of the entire survey is the resources that organizations are allocating to compliance activities. Eighty-four percent of the organizations indicated that they are allocating 20% or more of their valuable engineering resources to addressing compliance-related activities. Often, it is because these resources are the only ones in the organization that are capable of identifying and locating the data, or they are the SME that can make sense of complex compliance controls. Regardless, compliance is a massive drain on valued resources, and organizations would do well to understand the impacts of those controls when prioritizing staffing and projects.

Working with a vendor that has full-stack solutions for data security and compliance is highly recommended. Data compliance continues to be a top priority for organizations of every size and finding the right data security tool that works across environments including web and SaaS apps, email and your hybrid, multi-cloud infrastructure to minimize risk and streamline compliance should be a main consideration of organizational leadership.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT analyst research firm that specializes in going "beyond the surface" to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4446.081324