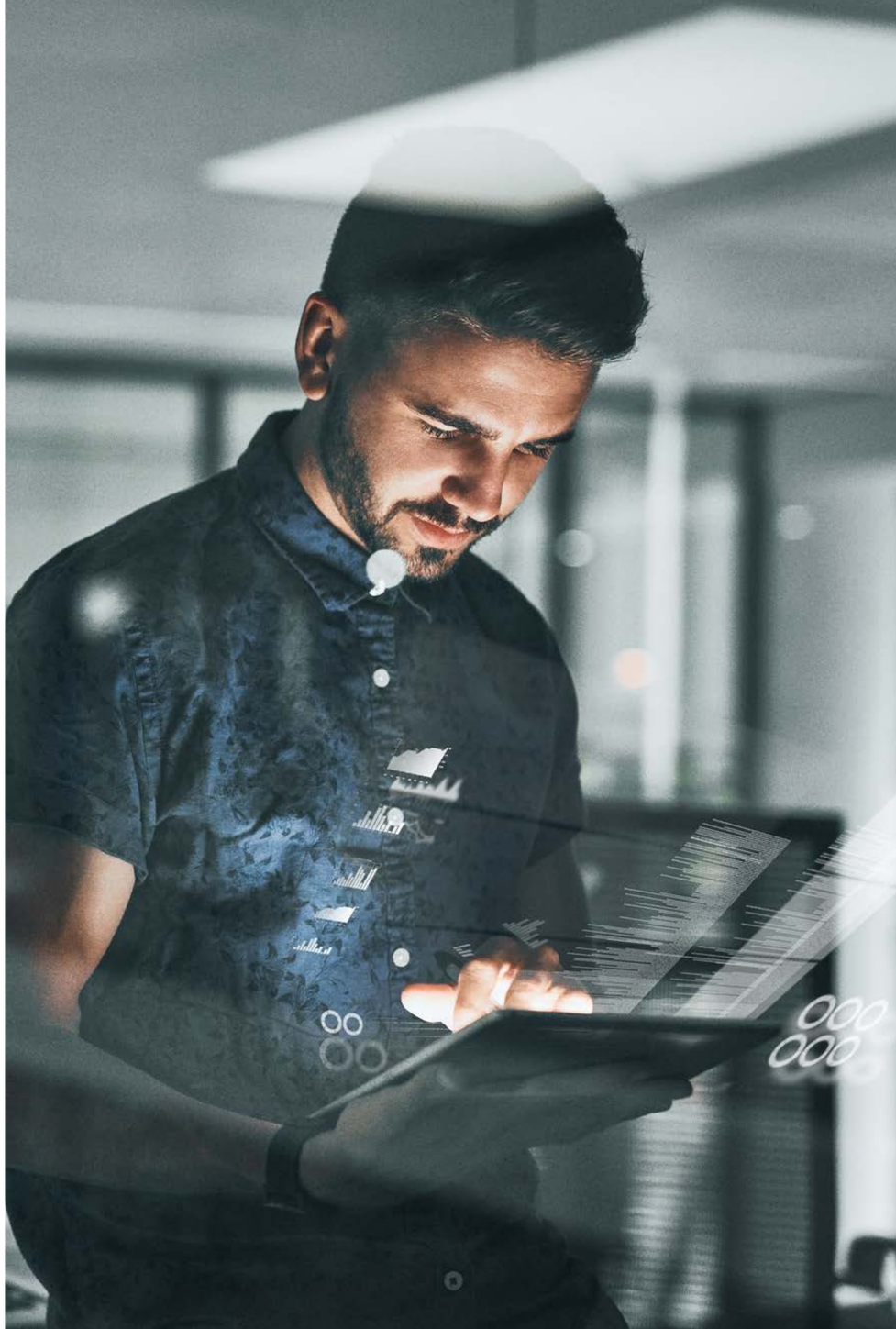
Enterprise Strategy Group™ by TechTarget

The Need for Data Compliance in Today's Cloud Era

Jack Poller, Senior Analyst

APRIL 2023

CONTENTS



Data compliance is foundational for digital transformation success

Digital transformation is driving bold business operational changes. According to the *2023 Technology Spending Intentions* research report from TechTarget's Enterprise Strategy Group, 77% of organizations reported that they are in the process of digitally transforming their business.

An essential ingredient of digital transformation is a modernized technology stack that uses public cloud services for greater agility. In fact, 46% of organizations have now adopted a cloud-first policy for new applications.

The democratization of cloud resources has enabled organizations to scale and innovate quickly. Organizations have used proprietary, shared and public data in the cloud to build higher-value customer applications. While organizations have strategically and operationally benefitted from the cloud, cloud usage has created a data challenge for many. Data sprawl across clouds, data use across multiple applications, and data's ability to transcend users have made identifying, cataloging and securing sensitive data difficult.

In addition, as a downstream effect of this trend, data compliance requirements that safeguard the handling and access to data have been put in place by various agencies. The burden of meeting these compliance requirements rests squarely on the enterprise, with significant fines and time-consuming audits for those that fall behind. So, while digital transformation might be the key to enterprise growth, meeting data compliance needs in this digital journey is the foundation of this success.

Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.

BACK TO CONTENTS

Cloud infrastructure becomes the default for running applications

The cloud has enabled organizations to develop applications to solve specific business problems rapidly. In addition to most applications already running in the cloud, enterprises report that they plan to move even more on-premises applications to the cloud.

Business applications in use worldwide

53%

of organizations have at least 500 business applications deployed worldwide.

Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey,* November 2022.

55%

of data and workloads currently run or operate in the cloud.

43%

of current on-premises apps will likely move to cloud in the next 5 years.

Source: Enterprise Strategy Group Survey Results, *The State of Data Privacy, Compliance, and Data Security,* October 2021.
Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey,* November 2022.

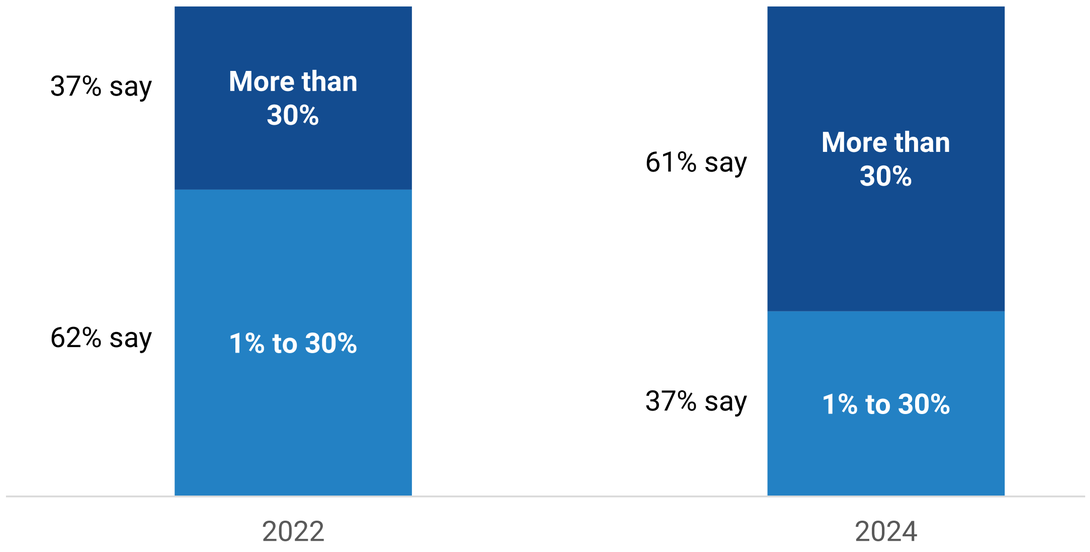
BACK TO CONTENTS

Data democratization is driving up the volume and the risk of cloud-resident sensitive data

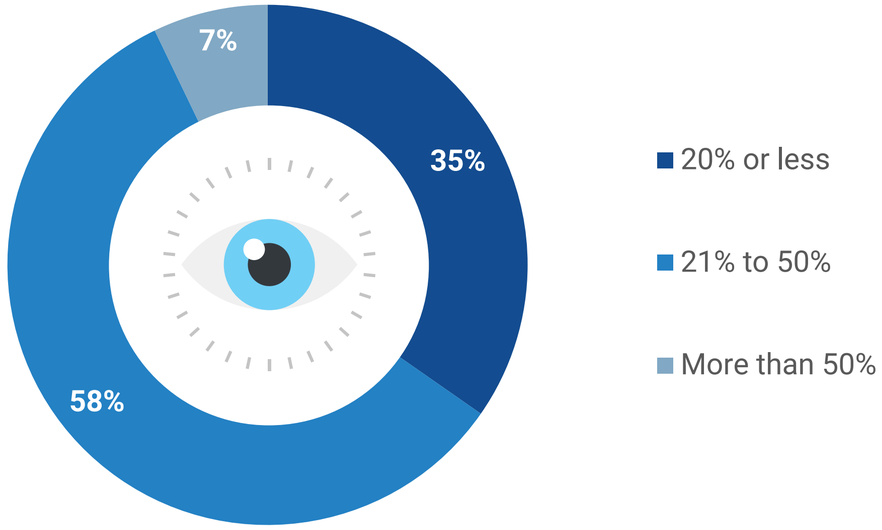
Data democratization has enabled more users and applications to interact with large volumes of data using user-friendly tools, interfaces, and APIs. While this has created value for the end user, it has created a security and compliance challenge for the enterprise. More users accessing more data without proper controls means a higher risk of data breaches and compliance issues. This challenge will be even more elevated as enterprises shift more sensitive data to the cloud over the next few years.

However, the complexities associated with the cloud have made it challenging for enterprises to adequately secure their data in the cloud. Controls that monitor, report, and autonomously respond to data access are the foundation for securing and meeting compliance needs. These controls need to be extended to sensitive data, as that represents the most significant risk to the enterprise.

Percentage of sensitive data that is cloud-resident



Percentage of cloud-resident sensitive data that is insufficiently secured



Source: Enterprise Strategy Group Survey Results, *The State of Data Privacy, Compliance, and Data Security*, October 2021.

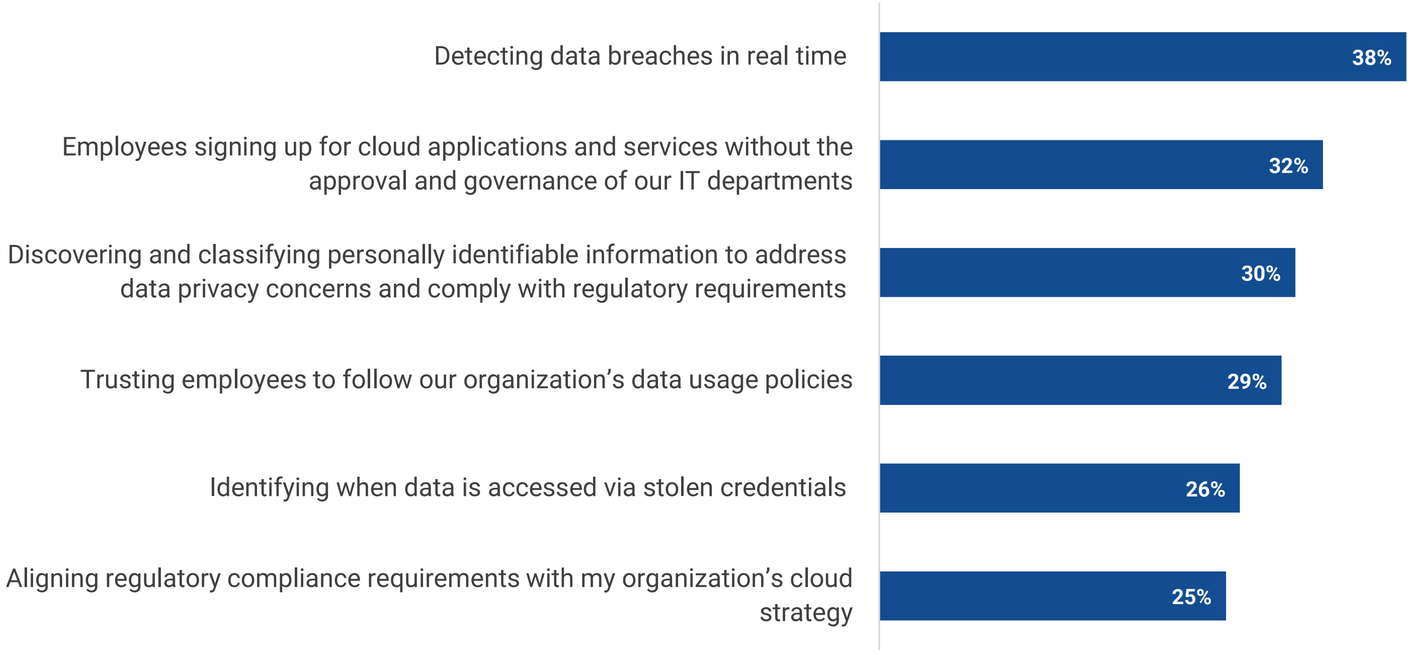
BACK TO CONTENTS

The increase of cloud-resident sensitive data is creating compliance challenges and security issues

Security and compliance are often characterized as two sides of the same coin—you can't have one without the other. As cloud-resident data increases, it raises the ante for the organization to secure ever-growing data and meet compliance requirements.

It's concerning that one-third of organizations have had cloud-resident data exfiltrated and lost through a breach. Of even graver concern, however, is that more than one-quarter of organizations think they've lost data through exfiltration but don't know for sure. This is most likely attributable to inadequate data security controls and expertise and implies a corresponding inadequacy in compliance.

The top six most significant data security challenges



Has your organization lost cloud-resident data?

33%

Yes, we know we've lost cloud-resident data

28%

Maybe, we suspect we have lost cloud-resident data

38%

No, we know that we have not lost cloud-resident data

Source: Enterprise Strategy Group Survey Results, *The State of Data Privacy, Compliance, and Data Security,* October 2021.

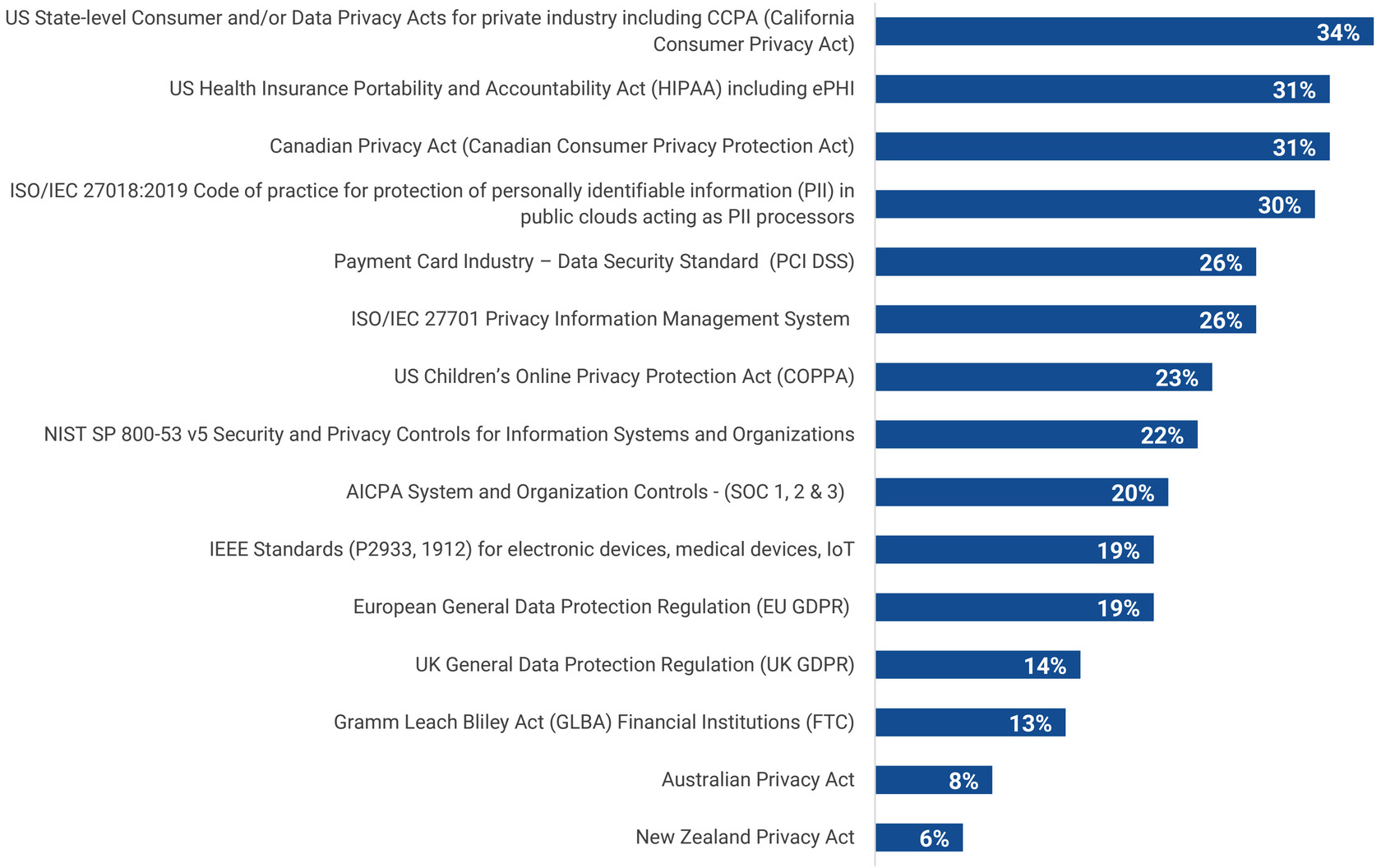
BACK TO CONTENTS

Organizations must comply with a broad range of regulations

Organizations need to comply with a multitude of regulations and laws, many of which are overlapping and contradictory. For example, CCPA, HIPPA, and GDPR have different definitions for what type of information needs to be protected, different reporting timelines in the case of a breach and different audit requirements.

As the consumers and oversight agencies have become more concerned about data security and privacy, the regulations have grown in complexity and the cost of violations has become more severe. Cloud data sprawl has only added more challenges to these compliance requirements.

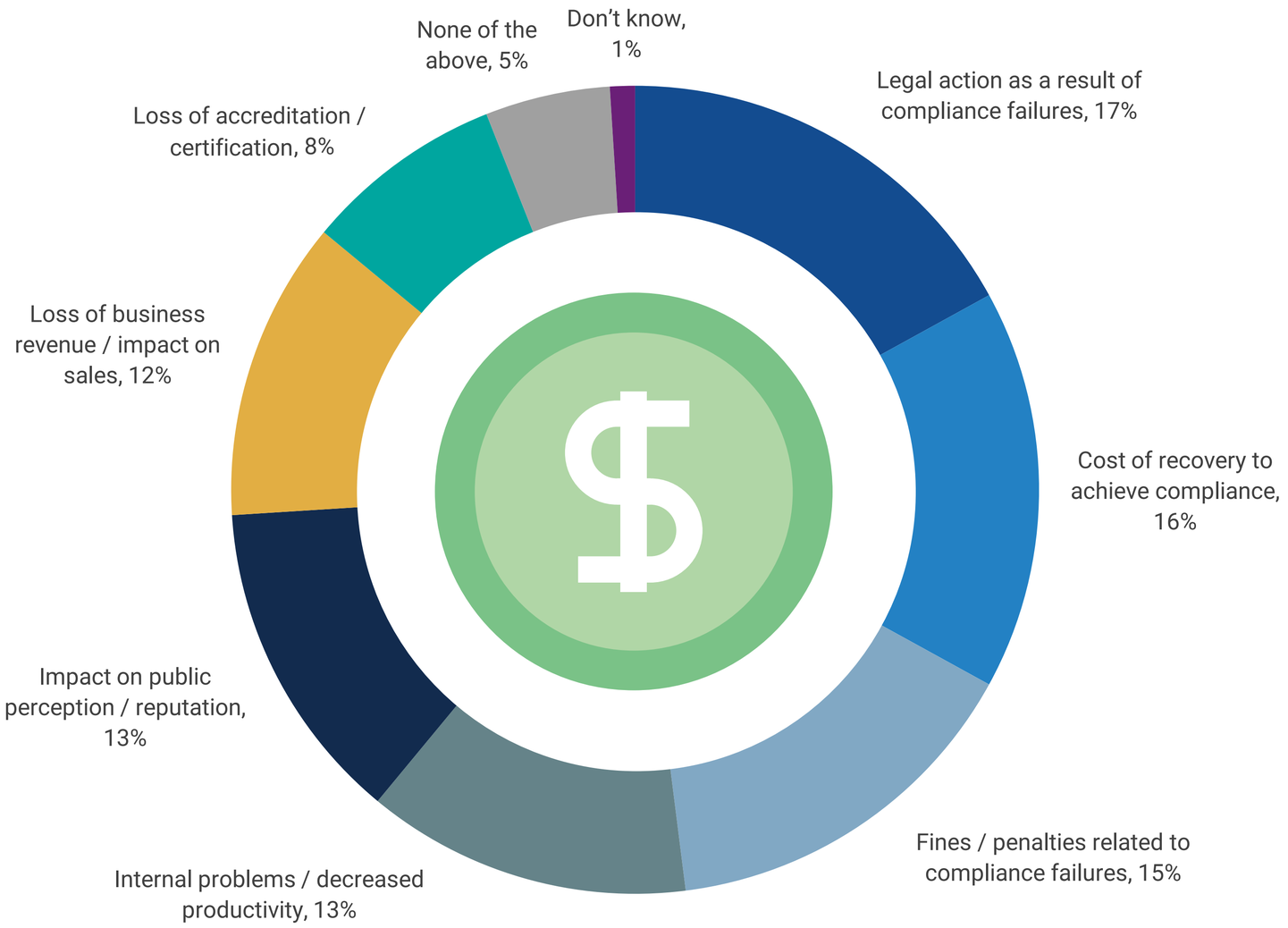
Percent of US organizations subject to data security and privacy regulations



Source: Enterprise Strategy Group Survey Results, *The State of Data Privacy, Compliance, and Data Security*, October 2021.

BACK TO CONTENTS

Area of greatest concern as reported by enterprises related to noncompliance



The painful reality of noncompliance

Under pressure from consumers, legislators have increased noncompliance fines to motivate businesses to protect data privacy and security. For example, GDPR penalties can be up to 4% of the business' annual worldwide turnover.

In addition to fines, organizations face additional noncompliance burdens, including reputational damage and legal consequences. Organizations also need to shift internal resources to quickly remediate issues exposed by audits, imposing both direct and indirect costs. This can lead to an interruption of critical, revenue-generating business activities.

No single noncompliance concern leads substantially, which suggests that a combination of factors impacting the whole organization arises from failing an audit.

Source: Enterprise Strategy Group Survey Results, *The State of Data Privacy, Compliance, and Data Security,* October 2021.

BACK TO CONTENTS

Privacy and compliance programs are staffed and mature

Organizations' compliance programs follow this journey to maturity:

Nonexistent
Lack of compliance controls

Just beginning
Impromptu controls

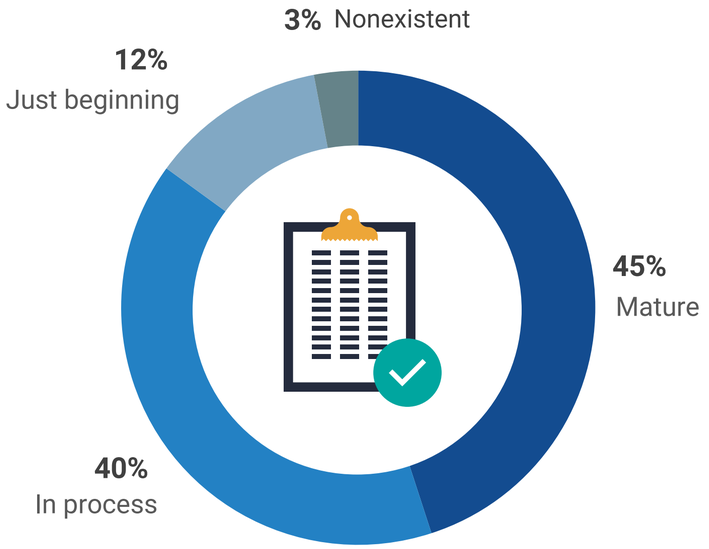
In process
Well-defined and managed controls

Mature
Optimal and independently verified controls

Newer companies have to rapidly implement compliance programs for all their subject regulations. Older, more mature companies will have had time to develop a program for older regulations such as the HIPAA privacy rules, which went into effect in 2003. These older companies will only need to make adjustments to their compliance programs for newer regulations such as the Virginia Consumer Data Protection Act (VCDPA), which went into effect in 2023.

Regardless of the type, size or industry, almost all businesses are subject to some level of regulatory oversight. This forces organizations to staff and build compliance programs, with 52% of organizations reporting that they have sufficiently staffed compliance programs.

Compliance program maturity



52%

of organizations on average **have sufficiently staffed compliance programs.**

Source: Enterprise Strategy Group Survey Results, *The State of Data Privacy, Compliance, and Data Security,* October 2021.

BACK TO CONTENTS

Organizations have a compliance confidence gap

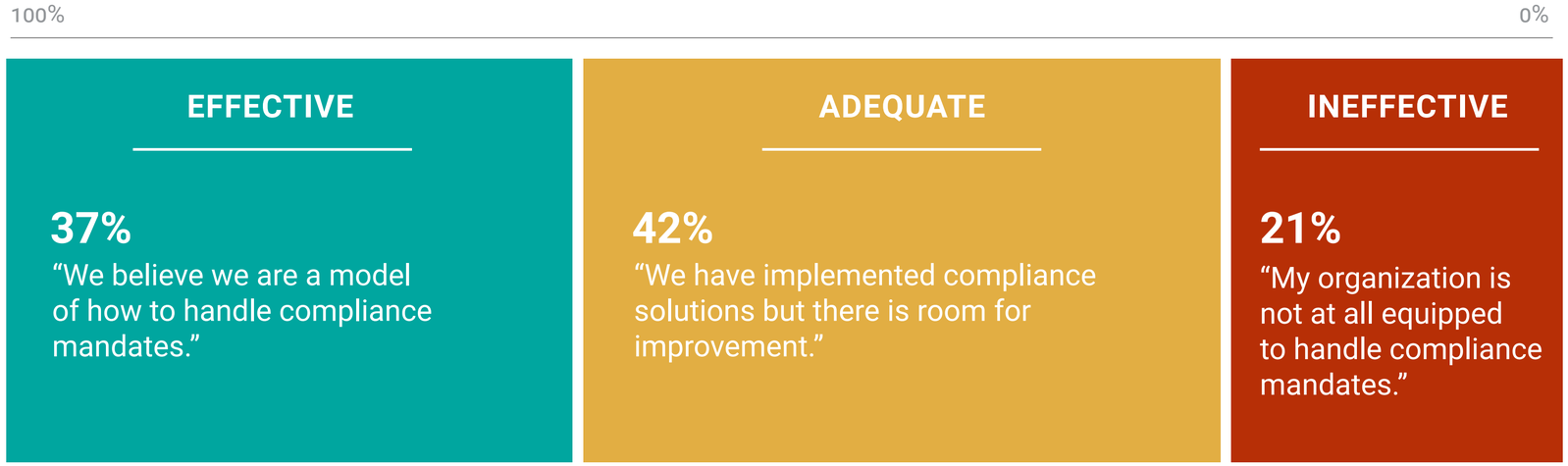
Despite having sufficient staff and mature programs, just over one-third of organizations are highly confident in the effectiveness of their data privacy and compliance programs. The remaining organizations believe that there is room for improvement.

What's driving this disconnect?

For more than half of organizations, the complexity introduced by shifting workloads to the public cloud has also made meeting compliance obligations more difficult. More users accessing more data in the cloud creates a challenge for enterprises in monitoring who is accessing what, why and where that data is stored. This decreases visibility, making compliance more demanding.

However, over one-quarter of organizations say that the cloud makes compliance easier. These companies likely use cloud APIs to programmatically and automatically identify, scan, index and classify all data stores, reducing the challenges introduced by cloud complexity and data sprawl.

Effectiveness of compliance programs



Public cloud impact on compliance obligations

52%

of organizations say the complexity introduced by shifting workloads to the public cloud **has also made meeting compliance obligations more difficult.**

28%

of organizations say that the **cloud makes compliance obligations easier.**

Source: Enterprise Strategy Group Survey Results, *The State of Data Privacy, Compliance, and Data Security,* October 2021.

BACK TO CONTENTS

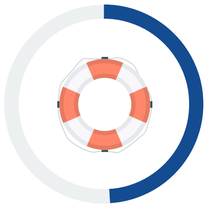
Organizations have various disparate tools deployed to help meet their security and compliance requirements

Organizations have put various technologies to work that help secure their data and ensure compliance. With the shift to the cloud driving complexity and decreasing visibility, organizations have deployed tools to help with everything from detecting data leaks to discovering unknown data sources and encrypting data. These data security-focused solutions help increase visibility, auditability, and security and support compliance reporting needs.

However, as the complexity of compliance requirements grows, many organizations need a comprehensive solution that brings together data silos to protect data and simplify compliance. These solutions will help narrow the compliance confidence gap that enterprises have.

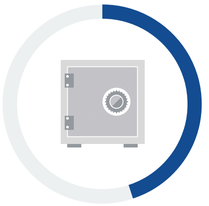
Usage of enterprise data security technologies

58%
Data backup and recovery



49%
Disaster recovery solutions

46%
Data in use

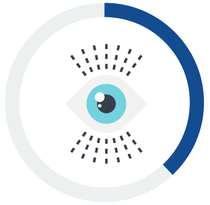


45%
Data leak/loss prevention

42%
Data discovery

41%
Data in transit

40%
Data classification



38%
Content inspection

38%
Data at rest

36%
Key management-as-a-service

Source: Enterprise Strategy Group Survey Results, *The State of Data Privacy, Compliance, and Data Security,* October 2021.

BACK TO CONTENTS

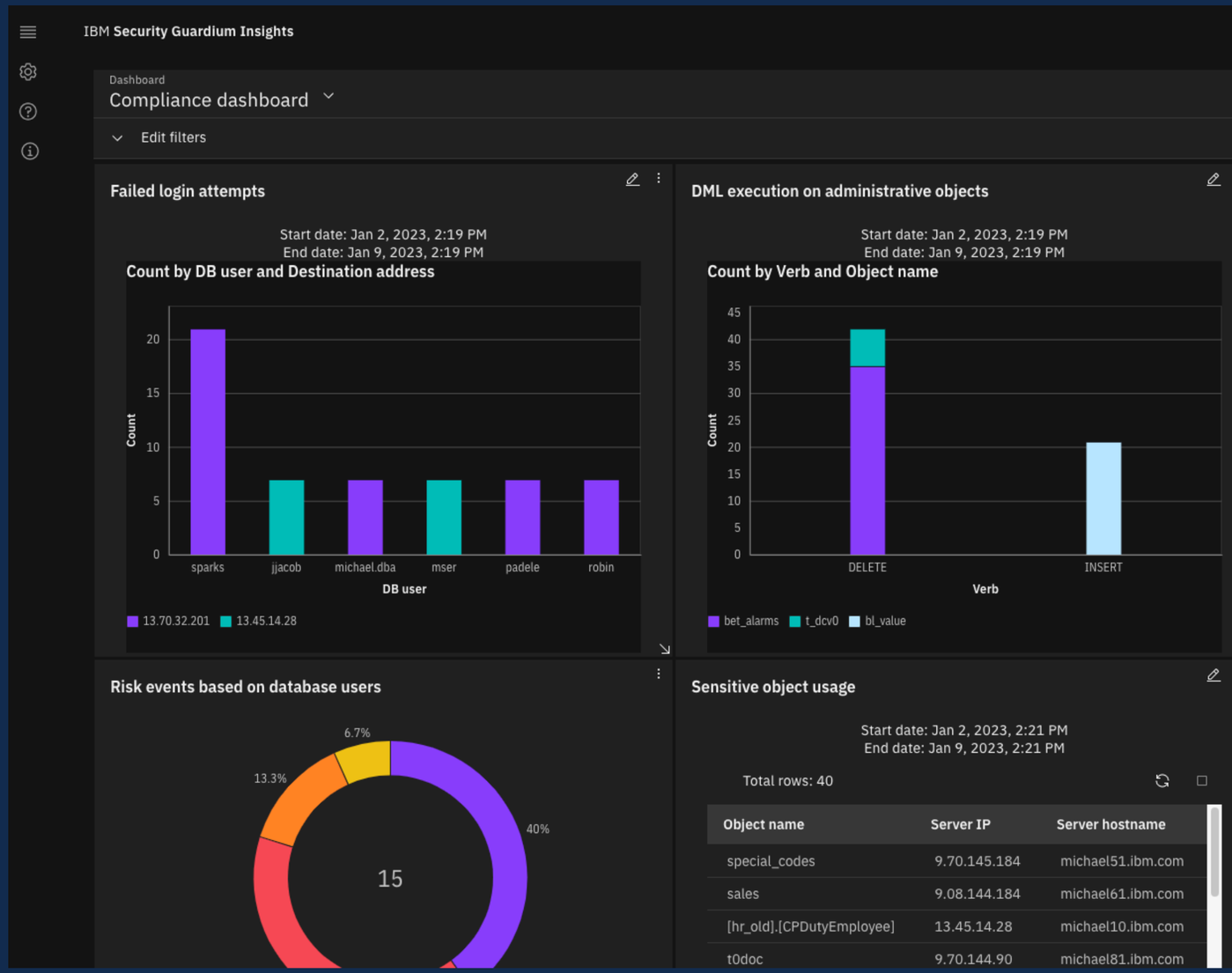
Conclusion

The transition of apps, workloads, and sensitive data to the cloud has brought about new security and compliance challenges for organizations. As data is scattered across hundreds, if not thousands, of silos, identifying, classifying, and securing data, as well as ensuring proper access and compliance with regulations, becomes increasingly difficult.

To address these challenges, organizations require a comprehensive data security platform that can locate and protect data regardless of its location. IBM Security Guardium has a proven track record of delivering comprehensive data security and compliance at scale. With the addition of new analytics and risk-based user experience, Guardium Insights is a powerful tool for organizations seeking to improve the efficiency and effectiveness of their data security program.

IBM Security Guardium Insights' robust capabilities allow enterprises to automate compliance policy enforcement and centralize data activity from multiple clouds. This enhances visibility and enables a consolidated view of how critical data is being accessed and used across hybrid environments. With IBM Security Guardium Insights, any enterprise can rapidly address its data security and compliance requirements.

LEARN MORE



BACK TO CONTENTS

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.