5 Data Governance Best Practices for 2021

The challenges of 2020 have required organizations to adjust their focus moving forward. Millions of workers have switched to remote work, a trend likely to continue long-term. At the same time, the expansion of data privacy regulations in an era of big data creates additional challenges. The data governance best practices listed below can help you stay on top.

Data governance incorporates the processes and rules that guide the use of information, thus helping to ensure that users have access to quality data. Some benefits of data governance include increased productivity, reduced risk and simplified regulatory compliance.

1. Structure Data for Remote Work

Following the lead of Silicon Valley tech giants, many organizations intend to keep workers remote, even after the pandemic. Consequently, they need to update data storage, access and transfer policies to increase data availability while reducing risk.

Remote work increases risk due to several key factors. Workers need the ability to find and use data from home with confidence in the quality of that data. At the same time, they often access and share data from personal devices and on networks that lack the robust security available in-house.

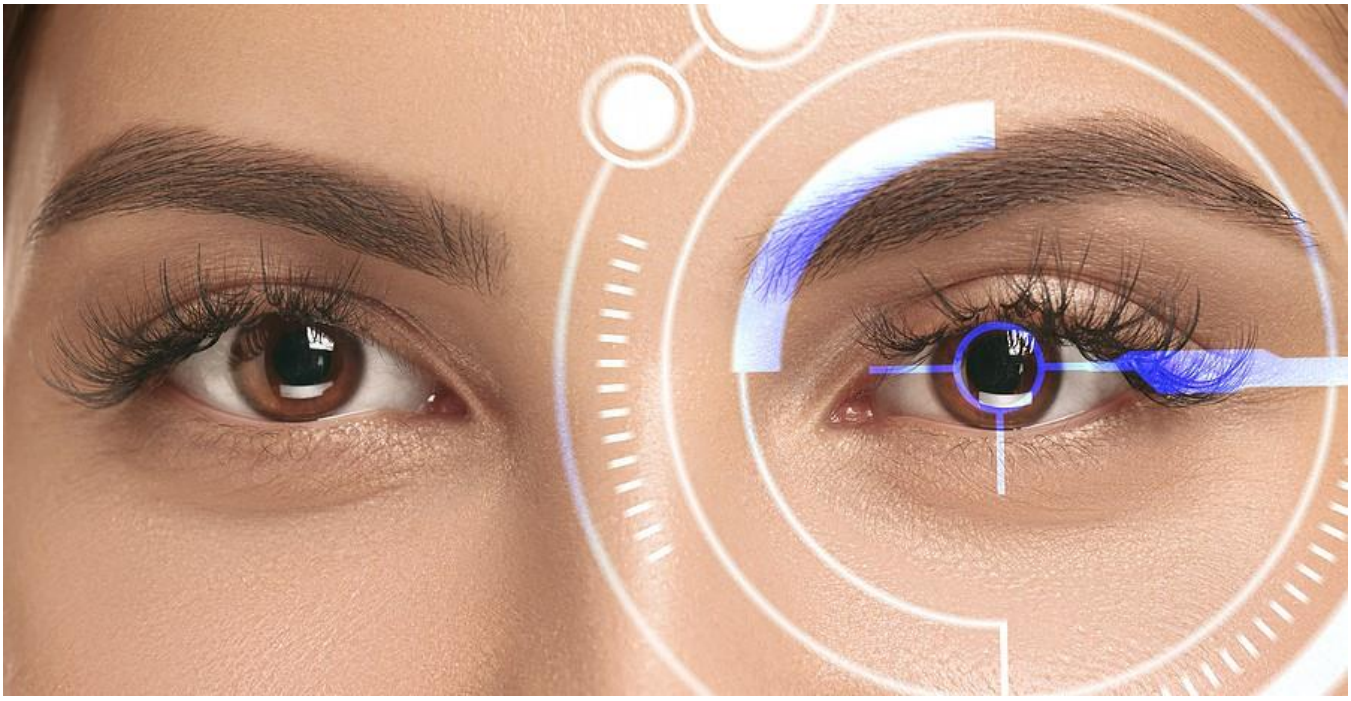
When the pandemic began, offices shifted to remote work almost overnight, sometimes taking risky shortcuts. Start the new year with an inventory of tools employees use to store, share and secure data from home. Then update processes and standards as necessary to balance usability with security and regulatory compliance. Provide user training and documentation.

2. Keep Shadow IT on the Radar

The switch to remote work has resulted in an increase in shadow IT. This includes the many applications employees use without IT knowledge or sanction to get their jobs done. For instance, employees may use unauthorized messaging apps to share sensitive data with coworkers. Or they may store company documents in personal cloud storage.

According to McAfee, the average organization uses 1,083 cloud services, and 975 of those fall into the realm of shadow IT. While many of those services may provide value, they also introduce security and compliance gaps. Additionally, use of shadow IT can disrupt workflows and result in corrupted data.

Organizations must educate employees on the risks of using unauthorized apps. At the same time, a regular inventory of shadow IT usage will help companies implement standards that can improve collaboration, efficiency and security.



3. Refocus on Basic Cyber Security

While cyber security tools continue to evolve, basic security best practices still apply. For instance, according to Microsoft, multi-factor authentication (MFA) prevents 99.9 percent of automated attacks.

Some additional cyber security best practices include encryption, mobile device management, regular backups, and network monitoring. While not new, these common-sense practices provide critical protection for sensitive data.

4. Incorporate a Data Privacy Framework

In essence, a data privacy framework involves documenting the practices and procedures around protecting sensitive data. It identifies those responsible for data protection, indicates how to assess risk,

how data will be stored and deleted and so forth. Essentially, it outlines the data governance workflows, policies and procedures.

In addition to supporting compliance initiatives, data privacy frameworks create the foundation for a robust privacy program. This can increase efficiency while inspiring consumer trust and providing a sense of structure.

To help organizations build their data privacy frameworks, the National Institute of Standards and Technology (NIST) published a set of guidelines in early 2020. This NIST Privacy Framework offers voluntary procedures to aid compliance and support privacy-by-design. It aims to help executives make informed decisions about data privacy.

5. Boost Data Literacy

Any list of data governance best practices this year should include data literacy. With an increasing emphasis on data-driven decision making, employees at all levels must be able to understand, evaluate and communicate data properly.

Consequently, organizations need to evaluate data literacy and build data literacy programs to address gaps. For example, do employees know how to evaluate data quality and test hypotheses? Can they translate data into charts as part of a compelling business case?

Data Governance Best Practices Save Time and Money

Implementing solid data governance best practices, organizations can increase efficiency and security, even in a remote work environment. Incorporating basic security and data privacy frameworks will also improve compliance with privacy regulations. And focusing on data literacy will empower organizations to gain the most value out of their data.

Messaging Architects provides the expertise to assist organizations with data governance, multi-faceted data security and compliance monitoring. We can help you harness the power of data to drive your business to new heights.