

Data governance for safeguarding data

So far, you've learned that data governance is a process that ensures the formal management of a company's data assets. The practices and policies in data governance ensure high data quality, management, and security within an organization. Organizations implement data governance policies when handling cloud data because of the data's inherent risks and vulnerabilities. In this reading, you'll learn more about the importance of data governance in safeguarding data, and how you can leverage technology to implement and support data governance policies.

The importance of data governance

Data governance in the cloud is critical to maintaining data security, quality, and compliance. Focused data governance policies ensure that data across networks is used and managed effectively, and that it's protected from potential threats like data breaches and unauthorized access. Data governance:

- Establishes strict access controls to ensure data security
- Ensures data's accuracy and reliability to maintain its quality
- Considers legal and business requirements for data storage and usage to ensure regulatory compliance

Define access control roles

To keep data secure, it's important for organizations to define roles and permissions for people who will be accessing their data. Usually, organizations will employ the principle of least privilege (PoLP), and grant the minimum levels of access, or permissions needed to accomplish a task. So, members of an organization only have access to the data necessary for their job. It's important to note that most organizations have policies against accessing data out of curiosity or lack of business reason.

While you may not be assigning roles and permissions as an analyst, your organization might take these aspects into account when defining roles:

- **Data owners:** The individuals who have authority over the data and decide who else can access it
- **Data stewards:** The individuals responsible for data management and quality
- **Data users:** End users – analysts like you – who need access to data to perform their roles
- **Administrators:** Individuals managing data security and access rights

Roles are clear, concise, and tailored to organizational needs, creating a sturdy foundation for data security and compliance.

Data stewardship processes

To maintain data governance, it's vital to establish and follow the data stewardship processes. As a reminder, data stewards are responsible for data management and quality. Effective data stewardship ensures that data remains a valuable and secure asset to an organization.

Data analysts usually immerse themselves in the details of the data, extracting insights and uncovering patterns. The close interaction analysts have with data makes them the best candidate to recognize inconsistencies, potential quality issues, and anomalies. It's important for data analysts and data stewards to have a collaborative relationship. Analysts support stewards in upholding the integrity and accuracy of data by communicating their findings. The feedback loop between data analysts and data stewards promotes a robust data ecosystem, ensuring quality issues are rapidly identified and addressed.

Data stewards:

- Manage data quality to ensure it's accurate, consistent, and reliable
- Oversee the entire data lifecycle, from its creation to its retirement
- Ensure lawful and ethical handling of data to maintain privacy and compliance

The role of technology in data governance

As an analyst, your team and organization will use a variety of tools to support data governance policies. For example, Looker is a business intelligence software and big data analytics platform that can be used to support data governance through various stages of data life cycles. Looker, and similar tools, support data governance by:

- Allowing users to create a centralized data model that ensures consistency and reliability across all utilized data
- Facilitating the creation of permission layers to control who can access the data, and to what level of interaction, establishing secure access boundaries
- Logging changes, access, and data usage to be audited, enabling tracking and review of data manipulation, and ensuring adherence to data governance policies
- Integrating various data warehousing solutions, allowing organizations to link their data management systems directly with the platform

Technology solutions that offer data governance software can be tailored to the specific needs of your organization. These tools have varying ranges of flexibility to ensure the features are aligned with organizational data governance policies and compliance requirements.

Key takeaways

Data governance is essential to ensuring that data is secure, reliable, and compliant with relevant regulations. Assigning specific roles with distinct permissions is crucial for maintaining a secure and functional data environment. A robust data stewardship process ensures data quality and lawful data management throughout the data lifecycle. Organizations can use technology like Looker to provide a structured, efficient, and secure method of managing data, adhere to governance policies, and enable insightful data utilization.

Resources for more information

Browse these resources for more information on data governance and best practices for implementing policies:

- [What is data governance?](#) details the benefits of implementing data governance practices, what data governance is used for, and how it relates to the cloud.
- [Best practices for data governance](#) provides an overview of data governance, and a few tips on best practices for implementing these policies.