

Data governance enables data teams to manage the overall availability, usability, integrity, and security of their data. five key data governance [principles to consider when designing a data governance framework.](#)

Why are data governance principles essential for business success?

Following data governance principles and implementing a successful data governance framework helps organizations manage and use data effectively to retain its value and reduces the risk of convoluted data operations. Data governance principles enable data teams to improve business and pipeline performance, reduce costs, and ensure compliance.

5 key data governance principles

Data security

What is data security?

Data security is the protection of sensitive or confidential information from unauthorized access or usage. It includes data encryption, secure data backup, access controls and permissions, and constant pipeline monitoring. These measures aim to ensure data confidentiality, integrity, and availability while protecting data pipelines from breaches or other cyber attacks.

Why is data security important for data governance?

Data security is essential for protecting organizations from information theft, legal disputes, financial losses, reputational harm, degraded consumer trust, and brand erosion.

How do you enforce data security in your data team?

Here are some steps you can implement to enforce data security in your organization:

- **Develop a data security policy:** Define what data is considered sensitive and establish guidelines for how your teams should protect it.
- **Conduct a risk assessment:** Identify potential vulnerabilities and threats to your organization's data and prioritize them based on their likelihood and impact.
- **[Implement access controls: Implement role-based access control for every data asset and limit access](#)** to only those who actually need it.
- **Encrypt all data assets:** Implement encryption across your data ecosystem to protect sensitive data from unauthorized access, both in transit and at rest.
- **Implement network security measures:** Use firewalls, intrusion detection, prevention systems, and other security technologies to protect your network from unauthorized access and attacks.
- **Regularly monitor and back up data:** Monitor and [audit](#) your systems and networks to detect and respond to security incidents. Furthermore, frequently back up important data to protect against data loss and ensure that it can be quickly restored during a disaster.
- **Keep systems up-to-date:** Regularly update software and systems to protect against known vulnerabilities.
- **Invest in security experts:** Consider outsourcing data security to experts, such as a managed security service provider, to ensure that all necessary security measures are in place and properly managed.
- **Create a security mindset:** Educate employees about data security policies and procedures and the importance of protecting sensitive information. For

example, you can simulate a real cyberattack scenario using red teaming to divide your employees into attackers and responders.

- **Post-incident handling:** Take the blameless approach to handle security incidents by focusing on recovery and understanding what went wrong and how to prevent similar incidents in the future.

Accountability

What is data accountability?

Data accountability is an organization's ability to take responsibility for the data it manages and owns. It encompasses several essential elements, such as the ability to explain the data, ensure its accuracy and completeness, govern it throughout its lifecycle, track its usage, and be transparent about its collection and use.

Why is accountability important for data governance?

Data accountability is necessary because it eliminates the back-and-forth communication needed to locate a data asset's owner.

Moreover, accountability helps promote trust in the data and the systems that use it, as well as the data teams. It can also help to prevent errors and data misuse.

How do you enforce accountability in your data team?

Here are some practices you can implement to enforce accountability in your data teams:

- **Assign roles and responsibilities:** Clearly define the data team members' roles and responsibilities and hold them accountable for their actions. Set examples by taking appropriate disciplinary action for violations of policies and procedures.

- **Assign owners to data assets:** Ensure all data assets have a clear owner to avoid unnecessary back-and-forth communication across teams.
- **Implement security measures:** Implement technical and organizational security measures to safeguard data from unauthorized access or breaches.
- **Encourage reporting and escalation:** Encourage data team members to report any concerns or violations of data governance policies and procedures.

Data integrity

What is data integrity?

Data integrity refers to data's accuracy, consistency, and completeness over its lifecycle. Several factors can affect data integrity, including software errors, hardware failures, human errors, and malicious cyberattacks.

Why is data integrity important for data governance?

Data integrity is a critical component for successful data governance as it ensures the reliability and trustworthiness of data. This is crucial for organizations to make accurately informed business decisions.

Without data integrity, organizations may be unable to trust the data they collect and use, leading to mistakes, errors, and loss of stakeholder trust. Therefore, data teams need data integrity to promptly detect and respond to data breaches, errors, or misuse.

How do you enforce data integrity in your data team?

Here are some of the best practices required for enforcing data integrity principles across your data teams:

- **Access logs and versioning:** Create access logs and implement versioning of data items so that all team members know who changed a data item, what was

changed, when it was changed, and where it was changed. You can use these logs and the version history as proof of data integrity.

- **Practice [referential integrity](#) for data validation:** Ensure accuracy and consistency across data tables with [pipeline data contracts](#) or foreign key constraints. Use data tests to validate the relationships between tables as a proactive approach to identifying and fixing issues.

Transparency

What is data transparency?

Data transparency refers to the ability of data teams and individuals to understand and access information about collected, used, and shared data. It includes information on what rights team owners and members have concerning their data. Data transparency also includes providing information about any data breaches, errors, or misuse.

Why is transparency important for data governance?

By providing a clear overview of all the data and its sources, data transparency lays a foundation for informed, thoughtful action. It empowers teams to find critical insights and avoid data bias in their decisions.

With access to all the data and the ability to see how it flows through the pipelines, transparency can help prevent data misuse and ensure that data is used in compliance with your data management policies.

How do you enforce transparency in your data team?

Here are a few ways to enforce data transparency within your data team:

- **Establish and document data policies and procedures:** Develop and document clear guidelines for data accuracy, completeness, and bias, as well as strategies for handling and protecting data.

- **Encourage transparent communication:** Assign data stewards to document and share data usage rules with team members and other stakeholders, including customers, employees, and regulators. Your teams can do this through [data contracts](#), transparency reports, or [data catalogs](#).
- **Conduct audits:** Regularly conduct data audits to ensure compliance with transparency standards and identify any potential issues.
- **Continuously educate and train the team:** Continuously educate and train the data team on the importance and best practices of data governance and management.
- **Open data lineage:** Empower data team members to trace data back to the source and identify biases and errors more easily with column-level [lineage](#).

Data quality

What is data quality?

Data quality is the degree to which pipeline data is fit for its intended use and meets organizational needs. It indicates the reliability of data across several key dimensions, such as accuracy, completeness, consistency, timeliness, and validity. Ensuring that these dimensions are adhered to leads to high-quality data.

Why is data quality important for data governance?

Poor data quality can lead data teams to incorrect conclusions, wasted resources, and lost revenue. Data quality directly impacts the accuracy and reliability of data-informed decisions, leading to improved business performance, reduced costs, increased efficiency, and enhanced customer satisfaction and credibility.

Data quality is particularly essential for organizations that must comply with regulations like data protection laws and those that handle sensitive personal information. Additionally, when different teams have access to consistent data, it's

easier for them to stay aligned on priorities, messaging, and branding, yielding more strategic, cohesive results.

How do you enforce data quality in your data team?

You can take the following steps to enforce data quality in your data teams:

- **Involve all data stakeholders:** Build a data governance council and make sure that top-level management is involved. For instance, data analysts can resolve many data quality issues through cross-departmental participation — for example, by ensuring the usage of correct data sources and calculating metrics according to business expectations.
- **Perform data cleaning:** Make sure your data stems from a verifiable source and goes through a cleaning process. Data cleaning includes eliminating duplicate records, correcting errors in data entry, and standardizing data formats.
- **Continuously monitor data quality:** [Data monitoring](#) should be a key factor of your data governance program. It involves ensuring that your data meets established standards while identifying and addressing any errors or inconsistencies. To achieve this you can use automated [data tests](#), set up alerts for failed tests, and create dashboards and reports.
- **Root cause analysis for data issues:** Address the root cause of every data issue, so your teams can prevent the problem in the future.
- **Maintain a data quality issue log:** Each issue needs an entry complete with information regarding the assigned data owner, the involved data stewards, the issue's impact, the final resolution, and the timing of any necessary proceedings.
- **Establish data quality indicators:** Define quality KPIs called data quality indicators (DQIs) that work together with general KPIs for business performance. You can

associate these metrics with data quality dimensions like uniqueness, completeness, and consistency.

Achieve reliable and secure data operations with data governance principles

Data governance is an essential process for achieving reliable and secure data operations. By implementing a data governance framework, organizations can ensure data quality, security, and compliance with legal and regulatory requirements. It also promotes a culture of transparency, accountability, and trust, which helps to build and maintain relationships with customers and stakeholders.

Implementing the five data governance principles above can help your data teams improve decision-making, reduce costs, increase efficiency, and protect sensitive information.