



The data governance blueprint

How to build a quality program





Table of contents

Introduction to data governance.....	Page 1
Establishing a data governance framework.....	Page 3
Data discovery and classification.....	Page 5
Implementation and technical controls.....	Page 6
Performance management and monitoring.....	Page 7
Preparing for what comes next.....	Page 9

An introduction to data governance



Effective data governance programs are essential but often lacking. Managing data from collection to disposal has become increasingly challenging. [Gartner reports that 80%](#) of organizations aiming to scale their digital business will fail due to poor data governance.

Data flows into an organization from various sources, including product orders, subscription sign-ups, customer surveys, employee interactions, and quarterly business reports. Each interaction generates additional data, increasing the complexity of data management.

Despite the importance of data governance, many organizations struggle with implementing effective programs. The ability to manage data through its entire lifecycle has become increasingly complex due to:

- **Volume and variety:** The sheer amount of data and its various forms (structured, unstructured) make it difficult to manage and govern.
- **Regulatory requirements:** Compliance with data protection laws and industry regulations adds layers of complexity.
- **Technological advances:** Rapid technological changes and the proliferation of new tools and platforms can outpace governance efforts.

To establish a successful data governance program, it should support and enhance organizational goals, driving value from data while adapting to evolving business needs, technological advancements, and emerging opportunities.

In this guide, we will cover how to:

- 1 Establish a data governance framework
- 2 Discover, classify, & understand your data
- 3 Implement technical controls that support governance policies
- 4 Manage and monitor your program performance

Foundations

The foundations of data governance are essential for managing data effectively and ensuring its quality, security, and compliance. They are:

Data stewardship involves the management and oversight of data assets to ensure they are accurate, secure, and used effectively.

- Data stewards are responsible for data quality, data definitions, and data policies. They ensure that data is properly classified, stored, and used according to organizational policies.

Data quality focuses on maintaining the accuracy, completeness, consistency, and reliability of data.

- It involves processes for data cleansing, validation, and enrichment. High-quality data is essential for making informed decisions and generating reliable insights.

Data security involves protecting data from unauthorized access, breaches, and other threats.

- This includes implementing measures such as encryption, access controls, and security policies. Ensuring data privacy and compliance with regulations (like GDPR) is also crucial.

Data compliance ensures that data management practices adhere to legal and regulatory requirements.

- It involves understanding and implementing laws and regulations related to data privacy and security. Regular audits and documentation help maintain compliance and address any issues.

These foundations create a robust framework for managing data effectively and ensuring it serves the organization's goals while protecting it from risks.

Quick guide to starting your data governance program

Transparency

Know what data you have, where it's located, what it contains, and how it should be protected.

Accountability

Who is responsible for your data, why do they have access to it, and what are they using it for?

Data Integrity

Is your data accurate, relevant, and timely? Does it follow policies? How can your data quality be improved?

Collaboration

Is there common ground for different disciplines within your organization to view, manage, and operate?

Establishing a data governance framework



Frameworks offer a strategic overview of the policies and procedures essential for effective data governance. Implementing a well-structured framework early on empowers organizations to navigate their extensive data assets more efficiently and make informed decisions about data management and protection. While data governance varies across organizations, certain key policy decisions are critical when establishing your framework:

Data classification

1

Data classification involves categorizing data based on its sensitivity, confidentiality, value, and regulatory needs. This enables organizations to apply suitable security measures, access controls, and handling procedures, ensuring a comprehensive understanding of data assets.

Retention schedules for regulated data

3

Retention schedules determine how long different types of data should be retained for legal, regulatory, or business purposes, and outline secure disposal guidelines. Collaborating with legal and compliance teams is advisable to establish internal guidelines.

Privacy regulation

2

With global data privacy regulations constantly evolving, organizations must adopt a strategic approach to their data governance. This includes understanding and adhering to regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), to ensure compliance.

Data mapping

4

Data mapping involves creating a visual representation of data flows within an organization. This process provides insight into data movement between systems and the relationships between data entities, highlighting areas for enhanced protection and identifying outdated or redundant records for removal or archiving.

Keep in mind

Just as a building requires a robust foundation, a successful data governance program relies on a well-structured framework. This framework is crucial for safeguarding your organization's most valuable asset: its data. The most effective way to develop a data governance framework is by applying the five Ws (and one H), which include:

WHO?

Identify the key stakeholders, data governance officers, and data stewards who are responsible for and impacted by the data.

WHERE?

Determine where the data is stored and managed. Understand the data architecture, which outlines the structure of data and related resources.

WHAT?

Define your data governance objectives and the metrics for measuring both short-term and long-term success. Specify what data will be collected, stored, and processed.

WHEN?

Establish timelines for data movement between stakeholders and the organization. Identify key intervals for data and metadata movement and determine when data should be disposed of.

WHY?

Clarify the purpose behind implementing data governance. Understand the mission driving this initiative and the reasons for collecting and utilizing data.

HOW?

Detail how data will be modeled and integrated into processes such as analysis, design, testing, maintenance, and security. Outline methods for managing consent and ensuring processes remain efficient.

Data discovery and classification



Manage your ROT data

Over time, organizations inevitably accumulate ROT data—redundant, obsolete, or trivial information that no longer holds significant value. ROT data often arises from factors such as inadequate maintenance, human error, or natural data degradation, expanding your organization's vulnerability to potential threats.

To mitigate risks associated with ROT data, it is crucial to implement a clear data retention and deletion strategy. Regular maintenance practices are essential for safeguarding data integrity and preventing the high costs and risks associated with retaining outdated information.

Monitor new and existing data

As new data integrates into your ecosystem, ensure it is accurately cataloged, added to your inventory, and that its consent and purpose align with your data mapping. Continuous monitoring of this data facilitates tracking across your entire infrastructure and identifying any deviations from expected data patterns.

By establishing a process to categorize data upon entry and automatically detect issues as they arise, you ensure that all critical data assets are identified, protected, and effectively governed.

Data lifecycle management

- **Delete the data:** Ensure timely disposal of data that no longer serves a purpose
- **Maintain transparency and purpose:** Clearly define where personal and sensitive data resides within your organization and ensure proper handling
- **Process personal data:** Manage personal data throughout your systems, including sharing with partners and vendors across borders

Implement a structured approach to store, process, and dispose of data, maintaining compliance and securing your data assets throughout their lifecycle.

Implementation and technical controls



While data discovery and classification determine the location and nature of your data assets, technical controls define how you govern them.

The most effective data governance programs integrate a security philosophy known as “shift left.” Rather than classifying data only after it has entered your ecosystem—when it is most complex and prone to errors—this approach focuses on data at the point of creation or collection. By addressing data governance early (at the left of the funnel), you can implement technical controls and classification processes that enhance efficiency and mitigate risks.

Technical controls enforce policies through:

- Access controls
- Encryption
- Data masking
- Data loss prevention (DLP)
- Backup and recovery
- Data retention policies
- Audit trails and logging
- Data quality controls

Privacy control best practices

The size of a single data point increases throughout its lifecycle due to usage, duplication, and analysis.

The shift-left strategy emphasizes managing data right at the moment of its collection (at the start of the funnel). This early stage is the ideal time to classify data and apply technical controls, setting the stage for greater efficiencies throughout its lifecycle.

A shift-left strategy may include:

- Classification systems that categorize sensitive or confidential records
- Applying appropriate permissions from the start to reduce the risk of data breaches
- Defining policies that specify how long records are kept before deletion
- Awareness programs to educate employees on proper handling of sensitive information

Performance management and monitoring



As data and regulatory environments evolve, maintaining a robust data governance program is a continuous process. To effectively track your program's progress, identify the key performance and compliance metrics that significantly impact your organization. Success in data governance—what leadership will focus on—is determined by how well the program meets its objectives and delivers tangible business outcomes. Here are some key metrics to monitor your data governance program:

Data compliance metrics

These metrics gauge how well your organization meets legal, regulatory, and internal policy requirements related to data management.

- **Number of policy violations:** Tracks the frequency of breaches or deviations from established data governance policies. This highlights where policies might have areas of weakness.
- **Adherence to data retention and deletion policies:** Measures compliance with established guidelines for how long different types of data should be retained and when they should be deleted. This reduces the risk of non-compliance and storage costs.
- **Rate of privacy requests handled within specified timeframes:** Monitors the efficiency and effectiveness in addressing privacy requests from individuals, such as data access or deletion requests. This reflects how well your organization responds to privacy regulations.

Data access and usage metrics

These metrics assess how well sensitive data is protected and used according to guidelines.

- **Time taken to grant or revoke access:** Measures the efficiency of your access management processes. Faster processing times indicate a responsive system for managing data access.
- **Number of unauthorized access attempts:** Tracks attempts to access data without proper authorization. A high number may suggest vulnerabilities or insufficient access controls.
- **Percentage of data accessed within approved usage guidelines:** Evaluates whether data is being used according to predefined guidelines and policies. This metric helps ensure data is not misused or accessed beyond its intended purpose.

Performance management and monitoring (cont.)

Data governance adoption metrics

These metrics reflect how well data governance practices are integrated into the organization's culture and operations.

- **Percentage of employees trained on data governance policies:** Indicates the level of awareness and understanding of data governance policies among employees.
- **Number of data governance-related incident reports:** Counts incidents or issues related to data governance practices. This can help identify recurring problems or gaps in the framework.
- **Rate of compliance with data governance processes:** Measures how consistently data governance processes are followed. High compliance rates suggest that governance practices are well-established and adhered to.
- **Employee feedback on data governance implementation:** Gathers insights from employees on the effectiveness of data governance practices and their impact. This feedback can help refine and improve data governance strategies.

Data quality metrics

These metrics evaluate the overall quality and integrity of your organization's data.

- **Data accuracy rates:** Measures the correctness of data. High accuracy rates indicate that data is reliable and trustworthy for decision-making.
- **Completeness rates:** Assesses whether all necessary data elements are present and accounted for. High completeness rates ensure that data is comprehensive and useful.
- **Occurrence of duplicate records:** Tracks the presence of duplicate data entries. Reducing duplicates helps maintain data integrity and reduces processing errors.
- **Data integrity violations:** Identifies instances where data has been corrupted or altered inappropriately. Monitoring these violations helps maintain the reliability and consistency of data.

Keep in mind

Regularly evaluating these metrics enables organizations to maintain compliance, enhance security, improve data quality, and drive continuous improvement in their data governance programs. This comprehensive approach ensures that data governance remains effective and supports the organization's overall strategic goals.

Preparing for what comes next



The road ahead

The effectiveness of a data governance program hinges on its ability to maintain stringent data control and security while delivering sustainable business outcomes.

Successful data governance involves several essential steps. It begins with establishing a robust program framework and conducting thorough data discovery and classification to gain a comprehensive understanding of your data landscape. Implementing technical controls early in the data lifecycle through a shift-left strategy is crucial for preventing security incidents and optimizing downstream efficiencies.

Ongoing monitoring of the data governance program through key metrics is vital for ensuring continuous progress and realizing the full value of your organization's data. By systematically evaluating these metrics, you can ensure that your data governance efforts remain aligned with business goals and effectively support data-driven decision-making.

Experian's data governance services and solutions provides complete data visibility and control so security and privacy teams know what sensitive data you have, where it lives, and how it's protected, to reduce data risk.

[Contact us today](#) to learn more.