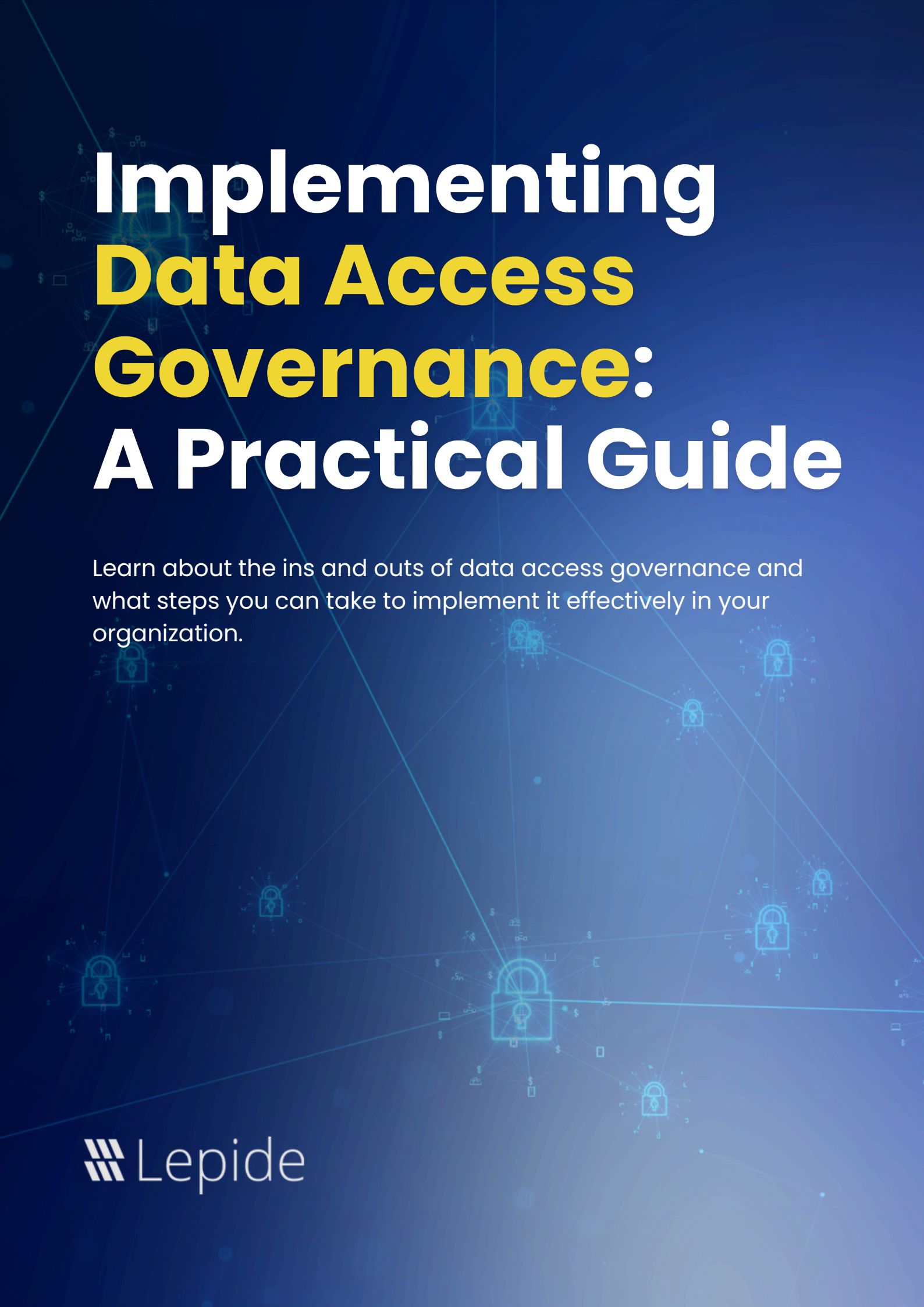
Implementing Data Access Governance: A Practical Guide

Learn about the ins and outs of data access governance and what steps you can take to implement it effectively in your organization.



Lepide

Say goodbye to complexity, and make effective unstructured data security a reality. It only takes 5 minutes to see how we do it!

- Lightning Fast Results
- Quick and Easy Integration
- Intuitive User Experience

Book Live Demo

Gartner peerinsights™

Lepide

Lepide

WHAT'S INSIDE

Introduction

In today's data-driven world, organizations are increasingly recognizing the value of their data as a strategic asset. However, the proliferation of data sources, coupled with the increasing complexity of IT environments, has made it challenging to effectively manage data access and ensure compliance with regulatory requirements.

Data access governance, a framework for managing data access and usage, is essential for organizations to protect sensitive information, maintain data integrity, and comply with relevant laws and regulations. By implementing effective data access governance, organizations can mitigate the risks associated with data breaches, unauthorized access, and misuse of data.

This whitepaper provides a comprehensive guide to implementing effective data access governance. It explores the key principles of data access governance, the benefits of adopting a data access governance framework, and the steps involved in implementing such a framework.

By following the guidelines outlined in this paper, organizations can establish a robust data access governance program that supports their business objectives and protects their valuable data assets.

Understanding Data Access Governance

Data access governance is a framework that establishes rules and procedures for managing access to data within an organization. It encompasses policies, processes, and technologies designed to ensure that only authorized individuals have access to the data they need to perform their job functions.

The importance of data access governance
Effective data access governance is crucial for several reasons:

- **Data Protection:** It helps protect sensitive data from unauthorized access, preventing data breaches and ensuring compliance with privacy regulations.

- **Data Integrity:** It maintains the accuracy and consistency of data by limiting access to only those who are authorized to modify it.

- **Regulatory Compliance:** It ensures compliance with industry specific regulations and standards, such as GDPR, HIPAA, and PCI DSS.

- **Operational Efficiency:** It streamlines business processes by providing employees with timely access to the data they need to make informed decisions.

- **Risk Mitigation:** It helps identify and mitigate risks associated with data breaches, unauthorized access, and misuse of data.

Key principles of data access governance

Effective data access governance is based on several key principles:

- **Need-to-Know Access:** Only individuals who need access to data for their job functions should be granted access.

- **Least Privilege:** Access should be granted on a minimum privilege basis, meaning individuals should only have the access they need to perform their tasks.

- **Separation of Duties:** Critical functions should be divided among different individuals to prevent fraud and unauthorized access.

- **Accountability:** Individuals should be held accountable for their actions regarding data access.

- **Regular Review:** Access rights should be reviewed regularly to ensure they remain appropriate.

- **Data Classification:** Data should be classified based on its sensitivity and value to the organization.

- **Access Controls:** Appropriate access controls, such as role based access control (RBAC) and attribute-based access control (ABAC), should be implemented.

- **Monitoring and Auditing:** Access activity should be monitored and audited to detect and respond to security incidents.

By adhering to these principles, organizations can establish a robust data access governance framework that protects their data assets and ensures compliance with regulatory requirements.

Assessing your current data access environment

Before implementing a data access governance framework, it's essential to conduct a thorough assessment of your organization's current data access environment. This assessment will help you identify existing vulnerabilities, gaps in your security posture, and areas where improvements can be made.

Identifying data assets

The first step in assessing your data access environment is to identify all of your organization's data assets. This includes:

Structured data

- **Databases:** Identify all databases used by your organization, including relational databases (e.g., Oracle, SQL Server, MySQL), NoSQL databases (e.g., MongoDB, Cassandra), and data warehouses.

- **Spreadsheets:** Inventory all spreadsheets used for data storage and analysis, including those stored in cloud-based platforms like Google Sheets or Microsoft Excel.

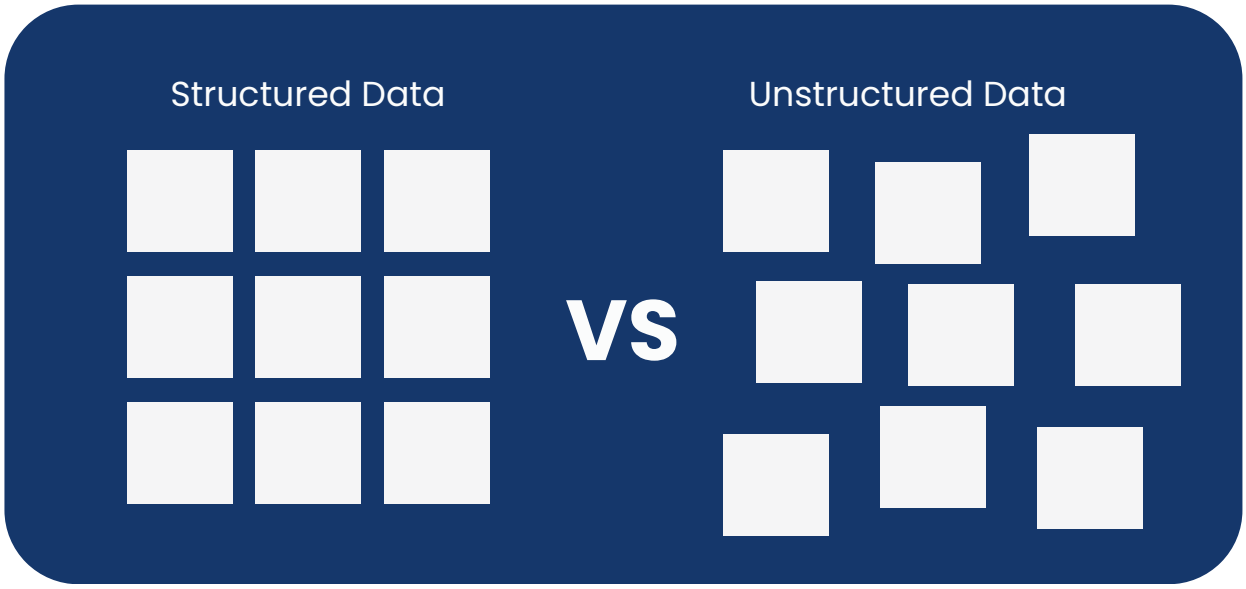
- **Other structured data repositories:** Identify any other structured data repositories, such as data lakes, data marts, or custom-built data stores.

Unstructured data

- **Documents:** Inventory all types of documents, including word processing files, PDFs, presentations, and technical drawings.
- **Emails:** Identify email servers and cloud-based email platforms used by your organization.
- **Images:** Inventory all image files, including photos, videos, and graphics.
- **Other unstructured content:** Identify any other types of unstructured content, such as audio files, social media data, and sensor data.

Sensitive data

- **Personally Identifiable Information (PII):** Identify any data that can be used to identify an individual, such as names, addresses, Social Security numbers, and credit card numbers.



- **Protected Health Information (PHI):** Identify any data that relates to the health of an individual, such as medical records, insurance information, and genetic data.

- **Other sensitive data:** Identify any other types of sensitive data, such as intellectual property, financial data, and government secrets.

Assessing current access controls

Once you've identified your data assets, you need to assess your current access controls. This includes:

Authentication Methods:

- **Password-based authentication:** Are passwords the primary method of authentication?

- **Multi-factor authentication (MFA):** Are MFA methods (e.g., SMS, push notifications, hardware tokens) used to enhance security?

- **Single sign-on (SSO):** Is SSO implemented to simplify user authentication?

- **Biometric authentication:** Are biometric methods (e.g., fingerprint, facial recognition) used for authentication?

Authorization mechanisms

- **Access control lists (ACLs):** Are ACLs used to define permissions for users and groups?

- **Role-based access control (RBAC):** Are RBAC policies in place to assign permissions based on roles?

- **Attribute-based access control (ABAC):** Are ABAC policies in place to assign permissions based on attributes (e.g., job title, department, location)?

Least privilege

- Are access rights granted on a minimum privilege basis?
- Are regular reviews conducted to ensure that users have only the access they need to perform their job functions?

Separation of Duties:

- Are critical functions (e.g., data entry, data validation, data access) divided among different individuals?
- Are there policies in place to prevent conflicts of interest?

Evaluating Compliance Risks

Finally, you need to evaluate your organization's compliance risks. This includes:

- **Regulatory requirements:** Are you compliant with relevant industry regulations (e.g., GDPR, HIPAA, PCI DSS)?Data breaches: Have you experienced any data breaches in the past?

- **Internal audits:** Have you conducted any internal audits to identify security vulnerabilities?

- **Third-party assessments:** Have you undergone any third-party security assessments?

By analyzing your current data access, you can pinpoint security risks and improve your data governance framework.

Developing a data access governance framework

Developing a data access governance framework requires a comprehensive approach that addresses both technical and organizational aspects of data security. This chapter outlines the key steps involved in creating a robust framework.

Establishing clear policies and procedures
The first step in developing a data access governance framework is to establish clear policies and procedures. These policies should define the organization's approach to data access, including:

- **Data classification:** A system for classifying data based on its sensitivity and value to the organization.
- **Access controls:** The types of access controls that will be used to protect data, such as role-based access control (RBAC) and attribute-based access control (ABAC).
- **Data retention and deletion:** Policies for retaining and deleting data to comply with legal and regulatory requirements.
- **Incident response:** Procedures for responding to data breaches and other security incidents.

Once the policies are in place, procedures should be developed to guide employees in implementing and following the policies.

- **Requesting access:** The process for requesting access to data.
- **Reviewing access:** The process for reviewing and approving access requests.
- **Revoking access:** The process for revoking access to data.
- **Reporting incidents:** The process for reporting security incidents.

Implementing role-based access control (RBAC)
Role-based access control (RBAC) is a common method for managing data access. RBAC assigns permissions based on a user's role within the organization. To implement RBAC, organizations should:

- **Define roles:** Identify the roles within the organization and the permissions associated with each role.
- **Assign roles to users:** Assign users to appropriate roles based on their job functions.
- **Review roles and permissions:** Regularly review roles and permissions to ensure they remain appropriate.

Implementing Data Classification and Labeling

Data classification is the process of assigning labels to data based on its sensitivity and value. Labeling data helps organizations implement appropriate security controls and ensure compliance with regulations. To implement data classification, organizations should:

- **Develop a classification scheme:** Create a scheme for classifying data based on factors such as sensitivity, confidentiality, and criticality.

- **Label data:** Label data assets with appropriate classification labels.

- **Review and update labels:** Regularly review and update data labels as needed.

Defining Data Retention and Deletion Policies

Data retention and deletion policies establish guidelines for how long data should be retained and when it should be deleted. These policies are important for compliance with legal and regulatory requirements, as well as for managing storage costs. To define data retention and deletion policies, organizations should:

- **Identify retention requirements:** Determine the retention requirements for different types of data based on legal and regulatory obligations.

- **Establish deletion procedures:** Develop procedures for deleting data that is no longer needed.

- **Implement data retention and deletion tools:** Use tools to automate data retention and deletion processes.

How to implement the framework

Implementing a data access governance framework involves a systematic, phased approach that ensures the right users have the right access to the right data. The first step is conducting a comprehensive data audit.

Organizations need to identify and classify their data based on sensitivity and importance. This process includes mapping out where data resides, who has access to it, and how it is being used. Tools that facilitate data discovery, classification, and access monitoring can be helpful in this stage, providing real-time visibility into data flows and access patterns.

Once the audit is complete, the next phase involves defining and enforcing access policies. Organizations should adopt the principle of least privilege (PoLP), ensuring users only have access to the data they need for their roles.

Role-based access control (RBAC) or attribute-based access control (ABAC) models can be implemented to streamline this process. These models automate access provisioning based on predefined user attributes or roles, reducing manual intervention and minimizing the risk of over-privileged access.

After establishing access policies, implementing continuous monitoring and auditing mechanisms is crucial. Organizations need to set up systems that can monitor user activity, flag anomalies, and generate alerts when unauthorized access attempts occur. Solutions that integrate with SIEM (Security Information and Event Management) tools can enhance the monitoring process, providing deeper insights into access trends and potential security risks.

The final step in the implementation process is regular review and adjustment. Access governance is not a one-time setup; it requires ongoing assessment to adapt to changes in organizational structure, user roles, and regulatory requirements.

Periodic access reviews should be conducted to verify that permissions align with current user needs, and de-provisioning should occur when users no longer require access. Additionally, organizations should stay informed of evolving compliance standards and update their framework accordingly to maintain adherence to industry regulations.

Data access governance solutions

Implementing a data access governance framework requires a combination of technical solutions, organizational processes, and training and awareness programs. This chapter outlines the key steps involved in implementing a data access governance framework.

Selecting the Right Technology

The first step in implementing a data access governance framework is to select the right technology. There are a variety of tools available to help organizations manage data access, including:

- **Identity and access management (IAM) solutions:** IAM solutions can be used to manage user identities, roles, and permissions.
- **Data loss prevention (DLP) solutions:** DLP solutions can be used to prevent sensitive data from being copied or transmitted outside the organization.
- **Data classification tools:** Data classification tools can be used to automatically classify data based on its content.

- **Data retention and deletion tools:** Data retention and deletion tools can be used to automate the process of retaining and deleting data.

When selecting technology, organizations should consider factors such as:

- **Functionality:** The tool should be able to support the organization's specific data access governance requirements.
- **Integration:** The tool should be able to integrate with the organization's existing systems and processes.
- **Scalability:** The tool should be able to scale as the organization's data and user base grows.
- **Cost:** The tool should be cost-effective and provide a good return on investment.

Integrating Data Access Governance Tools

Once the appropriate technology has been selected, it must be integrated into the organization's existing systems and processes. This may involve:

- **Connecting to data sources:** Integrating the tools with databases, file systems, and other data repositories.
- **Configuring policies:** Configuring the tools to enforce the organization's data access policies.
- **Integrating with IAM systems:** Integrating the tools with the organization's identity and access management system.

T**raining and Awareness Programs**

To ensure that employees understand and comply with the organization's data access governance framework, it is essential to provide training and awareness programs. These programs should cover topics such as:

- **Data classification:** The importance of data classification and how to properly label data.
- **Access controls:** The types of access controls that are in place and how to use them appropriately.
- **Incident reporting:** How to report security incidents and data breaches.
- **Best practices:** Best practices for data access and security.

Training and awareness programs should be ongoing and tailored to the specific needs of different employee groups.

Lepide

Data access governance best practices

By adhering to the following six data governance practices, organizations can eliminate data silos, improve data quality, and ensure compliance with regulatory requirements, ultimately leading to better decision-making and business outcomes.

Develop and Communicate Your Data Governance Program

A data governance program can help to overcome potential data governance obstacles such as limited resources, resistance to change, and lack of understanding. The process will involve effectively communicating the value and benefits of the program, providing training and support, and involving key decision-makers in the planning process. A data governance program can unlock measurable business value from your organization's data assets, while also ensuring data quality and integrity throughout its lifecycle.

Develop, Review and Update Data Governance Policies

A data governance policy is a set of guidelines that outlines the rules and standards for managing, handling, and protecting an organization's data. It ensures data accuracy, consistency, and security across the organization, and defines the roles and responsibilities of personnel involved in handling data. The policy outlines protocols for data collection, storage, processing, and disposal, and aims to improve data quality, enhance data security, and ensure compliance with regulatory requirements.

Regularly reviewing and updating governance policies is crucial as outdated policies can lead to inefficiencies, conflicts, and legal issues. Governance policies serve as the foundation for an organization's structure, operations, and relationships with stakeholders. Regular reviews and updates ensure that policies remain relevant, aligned with changing regulations, and reflective of the organization's evolving goals and priorities.

Additionally, reviewing policies promotes transparency, accountability, and inclusivity, as it encourages stakeholders to provide feedback and participate in the policymaking process.

Through regular reviews and updates, organizations can also identify and address potential gaps or vulnerabilities, thereby minimizing risks and ensuring a more resilient governance framework.

Conduct Regular Data Governance Training

It is crucial for all employees and executives to possess the skills to effectively understand, interpret, and use data to make informed decisions. This requires a fundamental understanding of what data is, its various applications, and the processes involved in collecting, storing, and managing it.

Additionally, learning how to work with data, including the use of visualizations, summaries, and descriptive statistics, is essential to effectively communicate insights and findings. Additionally, it is vital to recognize the limitations and appropriateness of data, as well as its potential biases and errors. By acquiring these skills, individuals can gain a deeper understanding of their role in safeguarding an organization's critical assets.

Gain Executive Buy-In Across the Organization

To successfully implement a data governance strategy, it's essential to gain executive buy-in across the organization. This involves not only demonstrating the benefits of data governance, such as solving specific pain points and improving business outcomes, but also aligning it with the organization's shared goals and objectives.

A production pilot project can be a key influencer, as it allows for tangible results to be presented early and often, and highlights the long-term importance of these wins. Once initial support is gained, it's crucial to maintain it by building trust and actively engaging executives through shared input and feedback. This enables them to feel a sense of ownership and commitment to the program. Data Governance is not just a technical issue, but a cultural and organizational change that requires buy-in from everyone in the organization.

Adhere to The Five Stages of Data Quality Management
Data quality management is crucial for organizations to make informed decisions and drive business growth. To achieve this, five stages of data quality management must be implemented.

Stage 1 – Migrate data to consolidate silos: Consolidate data from multiple sources into a single system to get a holistic view of your data and identify gaps.

Stage 2 – Validate your data: Implement real-time validation tools to prevent bad data from entering your system and ensure accuracy and consistency.

Stage 3 – Enrich your data: Combine internal and external data sources to make your data more detailed and valuable.

Stage 4 – Build and leverage a single customer view: Create a single, unified customer view by combining data from various sources to inform business strategies and marketing efforts.

Stage 5 – Routinely cleanse your data: Regularly review and update your data to ensure accuracy and relevance, and implement automated solutions to make this process efficient.

Use the Latest and Greatest Data Governance Tools

Data governance tools are essential for managing and maintaining data quality, integrity, and security throughout its entire lifecycle. Such tools enables organizations to discover, capture, and catalog data, as well as manage metadata, ensuring that data is properly tracked and protected from the moment it is created. Data governance tools also provides access control and data ownership capabilities, streamlining the daily tasks of the data governance team.

With advanced self-service tools and visualization, users can easily monitor and report on data usage, making it easier to identify potential issues. Look for solutions that allow for automated tracing of data sources and changes, provide a clear audit trail, and automatically apply data governance rules, ensuring compliance with regulatory requirements.

About Lepide

We founded Lepide back in 2015 because we felt cybersecurity was failing to keep up with the rapidly changing market. It lacked context and intelligence and was failing to protect what really mattered – the data.

Fast forward to today, and we have over 1,600 happy customers all over the world using our award-winning Data Security Platform.

Data breaches, including those associated with ransomware, often start with Active Directory, with attackers moving laterally within the network to target sensitive data in file servers and other data stores.

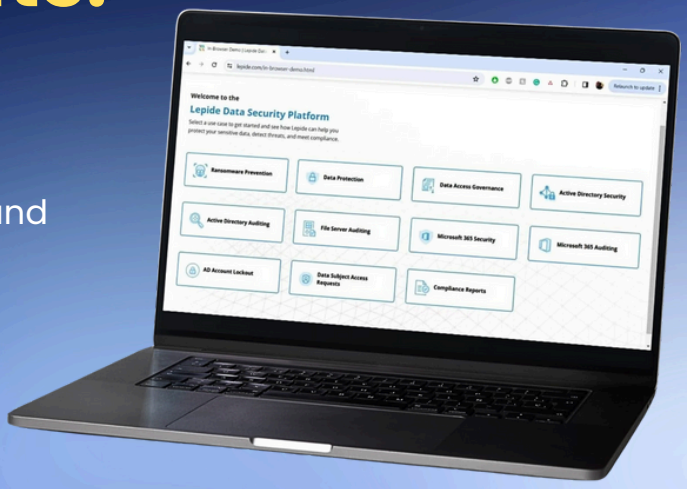
Our unique approach, and our powerful solution, provides the much needed visibility over changes to these critical systems and interactions with sensitive data. We deliver this information in real time to enable you to quickly detect and react to security threats.

The Affordable Game Changer: Lightning Fast Data Audits.

Try our FREE In-Browser Demo.

Analyze user behavior, secure data, and prevent threats in real-time.

Explore Today



Lepide

If you'd like to take a closer look at Lepide Data Security Platform, we recommend the first place to start is a personalized demonstration.

If you're more interested in detecting and preventing threats in your environment immediately, then we suggest to schedule a free risk assessment session with one of our security team.

Test Drive our In-Browser Demo Today!

Try Today

Ready to Explore More? Book a Call

Book Consultation

THANKS FOR READING

Lepide