

# Identity Governance Plus Data Governance is Today's Imperative



The business landscape continues to change rapidly. Organizations must strike a fine balance among productivity, cybersecurity, and privacy amid a data explosion. Additionally, new technologies drive exciting innovation but also bring risk. To thrive in this environment, companies need to find the right blend of identity governance and data governance.

## Business Challenges Require Careful Strategies

Today's IT team faces growing data-related challenges. For instance, data from digital marketing and the factory floor opens the door for valuable data analysis. However, managing that data and ensuring its quality and security requires detailed planning. Mismanaged data can result in flawed business strategy, information bottlenecks and security risks.

Meanwhile, migrating data and workflows to the cloud has increased collaboration and enabled [remote work](#). This allowed many businesses to weather the pandemic. At the same time, moving to the cloud means that security teams must now manage an exponential number of access points or risk data breach.

When organizations know where their data lives, as well as who owns and accesses it, they can build strategies to make quality data accessible to the right people at the right time. Enter data governance and identity governance.

## Unlock the Power of Digital Assets with Data Governance

Data governance includes the processes and tools relating to managing and securing data throughout its lifecycle. This involves properly categorizing and storing data while keeping it safe from ever-increasing cyber threats.

It also encompasses understanding regulatory requirements and achieving compliance while ensuring that decision makers have necessary access to up-to-date, high-quality data. And it includes planning for data end of life in a way that balances mandated data retention with purging or archiving outdated information.

Critical elements of a solid data governance strategy include the policies, rules and standards that determine how data is organized and shared. For instance, [retention policies](#) promote regulatory compliance and improve data quality. Likewise, sensitive data tags guard against improper sharing of privileged information.



## Streamline Access Management with Identity Governance

Identity governance works hand in hand with data governance by managing the users and devices that access the data. For example, when a new employee joins the organization, they gain a digital identity through which they access networks, folders, applications, and other resources. Likewise, devices such as laptops or printers also gain a digital identity.

Each user or device has an account in the system, and access controls determine what they have access to and what level of access they have. Passwords and other [authentication methods](#) allow users to verify their identities and gain appropriate access.

Thus, components of identity governance include account management and access controls, as well as authentication and password management. A quality identity and access management (IAM) system will automate much of these processes.

## Benefits of Complementary Identity Governance and Data Governance Strategies

When organizations incorporate identity governance in conjunction with data governance, they realize several key benefits, including:

- **Reduced cyber risk** – When users have the right level of access, protected by strong authentication measures and access monitoring, hackers struggle to find an open door. Likewise, increased visibility into data and users means that security teams can quickly detect and halt suspicious activity.
- **Improved compliance** – Proper categorization of data reduces the risk that users will share that data inappropriately. It also ensures that data will be retained or destroyed in compliance with regulations. Likewise, role-based identity governance helps achieve compliance by adjusting user access to match changing employee status.
- **Increased productivity** – When data is organized effectively and access is defined according to roles and responsibilities, users can quickly accomplish the task at hand. They no longer need to spend hours finding or re-creating information. Nor do they need to wait for IT to grant a critical access request or password change.
- **Informed decision making** – Access to quality data allows for effective data analysis. It also means that decision makers can strategize with confidence.



### Make High Quality Data Accessible to the Right Users at the Right Time

Implementing comprehensive identity governance and data governance strategies promotes collaboration and productivity while strengthening security and compliance. But building those strategies can prove complex.

Ease the process by partnering with the consultants at Messaging Architects. We combine extensive experience in [data management](#) and cybersecurity with detailed understanding of identity and access management tools.