Guidehouse
Outwit *Complexity*

# Mapping the Exploding Data Terrain with Good Governance Processes

## For organizations trying to navigate today's data sprawl, data governance is key to reducing the growing enterprise risk around data breaches, privacy violations, and data mishandling.

### What Is Data Governance?

Data governance refers to the internal capabilities—including policies, processes, procedures, standards, operating models, and technologies—an organization uses to ensure that the data it holds is stored safely, handled properly, remains trustworthy, and does not get misused. Data governance includes the development of policies around:

- Data creation and editing
- Data access
- Data storage
- Data usage
- Data maintenance
- Data quality
- Data inventories
- Data retention and destruction
- Organizational roles and responsibilities
- Cybersecurity

From data analytics to AI modeling, organizations now collect and use more data through their digital operations than ever before. As a result, many experience enormous increases in data volume, use, and storage. This data is often business critical, but it also has the potential to create significant problems if not handled correctly. And while data governance is not a new concern, the growing volume of internal and external data, how it is integrated, and how it is stored and secured make data protection and privacy the next big enterprise risk.

Most organizations do not have an enterprise-wide grasp of their data assets, where they are located, who can access them, and what regulations and rules govern their use and treatment. That data landscape will become more complex in the future, as data collection increases and emerging privacy regulations introduce unprecedented compliance challenges. The United States has hundreds of sector-specific data privacy and data security laws among its states. In March 2022, Utah became the fourth state to enact a comprehensive consumer privacy law, joining California, Colorado, and Virginia. As of May 2022, data privacy legislation was in committee in 11 other states. Additionally, the European Union, which led the way on data privacy and protection with the General Data Protection Regulation (GDPR), has two proposed laws to add more user protections and foster innovation, growth, and competitiveness. Rigorous data governance, protection, and privacy are necessary across the data life cycle to remain compliant and protect against reputational, regulatory, audit, financial, privacy, cyber, and access risks. But bad data governance also has a business cost. Indirectly, organizations might not be getting maximum value from their data to drive business innovation and revenue. Direct impacts to their costs can result from violations of privacy laws and regulations or data breaches. As an example, a lack of clear data destruction policies means companies often pay to store data they no longer need, increasing the risk of a data breach.

In 2020, the US Office of the Comptroller of the Currency fined a financial services firm $60 million for failing to monitor an outside vendor that was managing the company's data centers to ensure that customer data was handled properly. More and more, regulators are levying fines and penalties for data privacy violations, and with the introduction of new privacy regulations with more stringent requirements, organizations can no longer afford not to act on data protection and privacy.

The three tenets to managing this exploding data landscape encompass rigorous data governance, data access, and data usage practices. Data governance involves the capabilities—including policies, procedures, standards, operating models, and technologies—an organization uses to ensure the compliant and consistent handling of data by people, processes, and technology. Secure data access ensures that only those authorized and needing access to data are given that access. Proper data usage entails processes and rules that determine how data is used and handled. Here, we focus on the importance of data governance and on creating an effective data governance program, but this series also features papers focusing on issues related to data usage and data access.

### What Can Data Governance Help With?

Good data governance is critical for reducing risk to your organization and maximizing the value of its data. It can help your organization with:

***Improved business impacts:***

- Get maximum use of data for better business outcomes.
- Reduce data risks and costs by eliminating storage of unnecessary data.

***Better and more secure data access:***

- Enable more sophisticated role-based access to prevent accidental data misuse.

***Increased compliance:***

- Comply with current and prepare for future regulations.

***Improved security:***

- Ensure consistent data management practices.
- Clarify roles so all staff understand their responsibilities.
- Create access and identity management program guidelines.
- Reduce the potential for data breaches.

## The Importance of Data Governance

Organizations are increasingly becoming data-driven, but often do not have rigorous data governance capabilities in place to understand how best to handle data—why they have it, what they are using it for, where it should be stored, who grants access, who possesses business knowledge of the data, whether it is necessary, how it is accessed and secured, and where it can travel. This creates significant and varied organizational risks, including compliance, audit, and privacy concerns. For example, many data sources are subject to specific regulations, such as the European Union's GDPR guidelines or rules pertaining to data from clinical studies. Without clear data governance capabilities, data that falls under compliance rules might be moved to the wrong storage application or accessed by unauthorized people or for unapproved uses.

This multifaceted data landscape is even more complex because cybersecurity risks have increased in recent years with the adoption of cloud services, the internet of things (IoT), software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). When organizations store their data on other companies' platforms, it can create multiple layers of data security, data storage, data privacy, and data compliance issues that present further challenges. Data governance, including data protection and privacy, becomes a shared responsibility between the service provider and the organization. But many organizations do not have established cloud data governance policies to cover the access, usage, ownership, and security of externally stored data.

This increasingly complex data terrain requires organizations to develop data governing capabilities that ensure data is handled correctly and strategically across the data life cycle (i.e., the creating, editing, storing, distributing, maintaining, and destroying stages). Data governance is often handled primarily from a compliance perspective, but it should be seen instead as a pervasive, institution-wide concern that incorporates several functions and processes, including cybersecurity (e.g., identity and access management), business strategy, employee education programs, and change management. After all, data governance is not just an enterprise-level compliance program. It needs to reach throughout the organization to all those who work with data on a daily basis.

One common challenge to a robust data governance program is a lack of clarity around whose job it is to manage data and which functions should be involved in setting and implementing the data governing capabilities. Communication breakdowns or unclear roles and responsibilities are often to blame for breaches or privacy violations. Chief data officers, chief privacy officers, and chief information security officers should be at the forefront of data governance, working together—in collaboration with colleagues throughout the business—to ensure an effective and secure program.

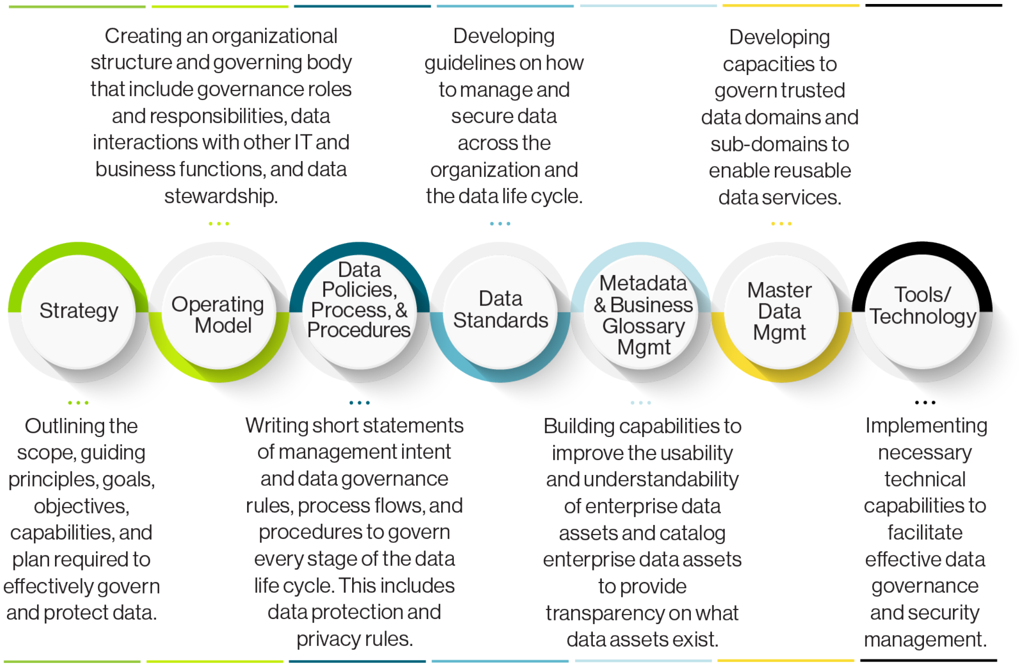
Data governance also needs to be handled culturally. It must be built into the mindset of every user and have a central place in the company code of conduct. Tackling such a wide-ranging, complex endeavor takes time. Given that new privacy regulations are likely to be implemented in the future, companies should prepare now to ensure that they have the cultural capabilities and institution-wide knowledge necessary to meet the data privacy and protection requirements of tomorrow.

Guidehouse
Outwit *Complexity*

## Guidehouse's Data Governance Strategy

Guidehouse has considerable experience working with government and corporate entities to support key internal stakeholders in developing, refining, and implementing effective data governance capabilities that both reduce enterprise risk and enable more trusted and reliable data to fuel mission and operational activities and decision-making.

We follow a seven-step data governance process:



Outlining the scope, guiding principles, goals, objectives, capabilities, and plan required to effectively govern and protect data.

Creating an organizational structure and governing body that include governance roles and responsibilities, data interactions with other IT and business functions, and data stewardship.

Writing short statements of management intent and data governance rules, process flows, and procedures to govern every stage of the data life cycle. This includes data protection and privacy rules.

Developing guidelines on how to manage and secure data across the organization and the data life cycle.

Building capabilities to improve the usability and understandability of enterprise data assets and catalog enterprise data assets to provide transparency on what data assets exist.

Developing capacities to govern trusted data domains and sub-domains to enable reusable data services.

Implementing necessary technical capabilities to facilitate effective data governance and security management.

## Conclusion

Guidehouse's deep data governance capabilities and expertise have helped many organizations improve their business operations by maximizing data usage while ensuring data protection and privacy to significantly reduce their risk.

By integrating enterprisewide data concerns and focusing on cybersecurity and privacy issues in a way that integrates data's value proposition and costs, Guidehouse helps organizations create a comprehensive data governance program with clear roles and responsibilities—and provides support throughout this crucial transformation. The resulting data governance capabilities create a strong foundation for organizations to successfully tackle the emerging complexity of data privacy and protection issues.

## About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures, focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 13,000 professionals in over 50 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit: **www.guidehouse.com**.

For more information,
please contact:

**Bob Audet**
Partner,
Data Management & Governance
raudet@guidehouse.com

**Michael Ebert**
Partner,
Cybersecurity
mebert@guidehouse.com

**Don Heckman**
Director,
Cybersecurity
dheckman@guidehouse.com

**Web:** guidehouse.com/cybersecurity / @GHTechSolutions linkedin.com/company/guidehouse-technology-solutions