Kevane Grant Thornton

Advisory

Business

Data governance

Upgrade your data governance

April 18, 2022

To effectively use and control data, businesses need effective data governance. The journey to effective data governance requires each business to identify its unique considerations, roles and rules that inform its principles of value and security.

Start with a focused approach and flexible framework

Any discussion of data governance should start with the business drivers for your company. Your industry, market position, business model, compliance requirements, strategies and other factors define your internal and external data demands.

You must keep your unique data demands in mind to ensure that your data governance framework is comprehensive enough for your enterprise while being specific enough to drive your strategies.

Assess your data risks

The risks to your data are real, and constantly evolving. If you do not have a formal data governance structure, with appropriate data security measures, your enterprise is at risk of data loss, operational disruption, regulatory non-compliance, and reputational damage. Risks arise from external attacks, access errors, internal negligence and more. An effective risk assessment identifies what can prevent you from achieving business goals, meeting compliance requirements, improving efficiencies or gaining competitive advantages.

As your data volume and structures proliferate, it's important to keep the following nine aspects of data governance risks in mind:

Strategic risks

1. data stewardship: your organization must have champions who are responsible for the quality and safety of data in each key function, or you can suffer a data breach in a critical gap where there is a lack of accountability and control.
2. organizational responsibility and communication: support your champions by establishing clear responsibilities and lines of communication.
3. data strategy: if your champions do not align their work with a formal data strategy, different business units may pursue conflicting agendas that undermine your data management overall.

Operational risks

4. data standards, policies, and procedures: even with the best strategy in place, data management will be inconsistent if standards, policies and procedures are not enforced. Insufficient guidance and enforcement will negatively impact data definition, collection, maintenance, use and security processes.

5. data architecture: your data strategy, standards, policies, and procedures should inform your data architecture. Make sure that you are housing data in a way that facilitates your current objectives and considers the flexibility that you are likely to need in the future.
6. regulatory compliance: poor data quality or ineffective data architecture can put your organization at risk of noncompliance fines and other measures, adversely impacting the organization's performance and reputation.
7. issue management: when questions arise about data quality, relevance, consistency, and availability, you need to be sure you can resolve them quickly and consistently.
8. project management: project management determines what gets done. Make sure that your data management work is effectively prioritized and funded.
9. data management services (vendor management): the success of your data governance is not entirely controlled by your employees. Make sure that your vendors are properly vetted, and that the terms of service are fully defined in the contracts.

Assess your data governance

Whether formal or advisory, a data audit can give you a holistic view of your data governance, providing essential transparency to executives and board members.

Below are some examples of the areas where a data audit can focus:

Maintenance

Effective data maintenance is essential for many reasons, including the need to ensure your data quality — which is a common concern, and a complex factor. Other factors impacting data quality might include accuracy — is the data the same after scrubbing, manipulation, and aggregation?

Security and access

Audits can look at network security, physical security, access security and authorization protocols. They can verify that controls enforce the principle of least privilege to all databases, data marts and data warehouses.

On the loss prevention side, an audit can help determine if a business needs — and is ready for — an automated loss prevention tool that finds and protects sensitive data. It can determine whether data is encrypted in all destinations, and in all states. Auditors can look at how data is classified by sensitivity, from public to highly compartmentalized. They can help determine if classifications are comprehensive and appropriate. They can also assess whether the necessary safeguarding procedures (such as encryption) are in place to protect the sensitive data.

Value

A holistic view of data emphasizes its power as a business tool. Here, many of the tools deployed to ensure data reliability, relevance and objectivity will be germane. Controls which ensure consistency, and rollback mechanisms which minimize duplication, will help decision-makers.

It's important to know where you are on your data governance journey, and where you want to be. It's also important to empower the people who can take you there.

Empower your people

Auditors identify and verify the conditions that will lead to your data governance program's success, but it is your day-to-day employees who create that success.

Your program's support must start at the top and permeate the organization. High-level support can take the form of a Data Governance Council, led by the Business Information Security Officer and the Chief Information Security Officer. The council should refine and

enforce the strategic vision of data governance across departments, tie that vision to larger organizational objectives, and serve as the escalation point for significant issues. Beside the council, designated data governance organization members would address the specifics of data management functions, data ownership and accountability across different areas and processes within the business.

Everyone within the organization is responsible for data governance. Employees, third-party vendors, contractors, and all other end users must access and use corporate data and information resources responsibly, and only for authorized purposes.

Leading practices and technology trends

Many of the high-level tasks in a data governance journey are common — start with a framework, assess your risks, assess your program, establish, and empower your roles. These form the foundation for a data governance program that aligns with your goals, identifies technology needs and informs ongoing assessments.

But the data governance landscape is rapidly evolving. Emerging tools can use AI and machine learning to streamline processes, reinforce data integrity, improve data visualizations, and enhance high-level storytelling that clarifies business decisions. At the same time, evolving ethical discussions mean that businesses will continually need to shift and address new issues.

Every business risk profile is unique, with different data demands at different stages on the data governance journey. To effectively store, transfer, manage, analyze, and secure data as the fuel for your business, form a holistic view on governance now and into the future.

Grant Thornton library articles:
Upgrade your data governance

We are committed to keep you updated of all developments that may affect the way you do business in Puerto Rico. Please contact us for assistance in relation to this or any other matter, we will be glad to assist you.

Marta Rodríguez
Partner Head of Advisory
E marta.rodriguez@pr.gt.com

Neysha Otero
Advisory Manager
E neysha.otero@pr.gt.com

Jorge Paredes
Advisory Manager
E jorge.paredes@pr.gt.com

Jorge Oquendo
Advisory Manager
E jorge.oquendo@pr.gt.com

Kevane Grant Thornton

grantthornton.pr