AN FTI TECHNOLOGY REPORT

A Pathway to Corporate Data Governance and Acquiring Value from Corporate Data Assets

Catalysts, Challenges, Approaches and Benefits

Scott Margolis, FIP, PMP, CIPP/US, CIPT
Dera Nevin, ESQ., CIPP/E, CIPP/US, CIPM

KEY TAKEAWAYS:

0101
0010
1010

Data is an asset class that attracts all of the obligations of any asset: corporate ownership, protection and loss prevention, and a clear understanding of the risk and regulatory obligations associated with maintaining and the disposition of the asset

All organizations should have a data catalog and thorough understanding of the data types the firm owns, licenses or acquires for current and future uses

Organizations will be enabled or constrained by their ability to use enterprise data in new and innovative ways. High-quality, authenticated and reliable data is a prerequisite for data monetization, machine learning activities, and enabling artificial intelligence initiatives

Organizations now recognize they have a new, powerful asset class at their disposal: their data and the information and actionable insights that the data constitutes. This asset class can provide significant returns and offers the potential to drive revenue, opportunities that have led corporate boards and C-suites in search of a path to monetize and derive greater value from corporate data. Even with this acknowledgement of value, however, many organizations are often at a loss for where to start or have made attempts at mining value through technology with unsatisfactory results. This paper covers the fundamentals of corporate data governance and explains why and how strong governance must be the foundation upon which value-add data programs are built.

Why data needs governance

The shortest path to the highest likelihood of success in realizing value from data is to establish a corporate data governance program. What exactly does this mean?

Data governance refers to the overall management of the availability, usability, integrity and security of data used within an organization. It involves the processes, policies, standards and guidelines that ensure data is handled in a consistent, controlled and responsible manner, from collection or acquisition through disposition. A key *objective of data governance is to establish a framework for a firm to manage data as a strategic asset class that is aligned with the organization's goals and objectives*. This includes establishing policies that facilitate data access, data availability, data quality, data security, data privacy with collection, acquisition and use policies that align to compliance with regulatory requirements.

Effective data governance involves collaboration among various stakeholders within an organization, including data owners, business users of data, IT teams, legal and compliance teams, and other specialized teams such as privacy, information security, and data science. By establishing a robust data governance framework, organizations can ensure that their data is accurate, relevant, consistent and trustworthy, which can improve decision-making, increase operational efficiency and mitigate risks associated with data breaches, incorrect use of data and regulatory non-compliance.

Beyond data governance, having a framework for managing data and associated enabling policies and procedures will facilitate an organization moving from data awareness to being able to determine and secure the value of its data, and take further steps to monetize and derive further value from this asset class, all while conforming to an array of regulatory and legal requirements.

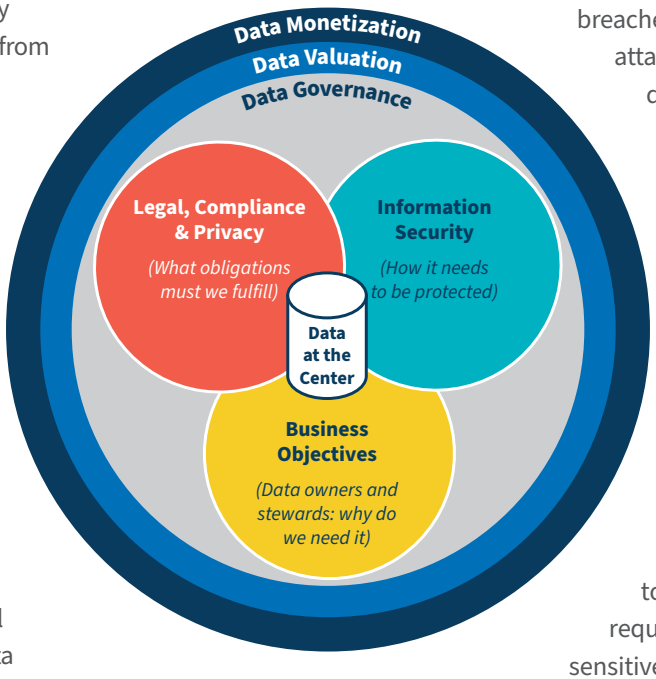
It all begins with data

A corporate data governance program must begin with a clear definition of purpose. Objectives should be discussed and agreed to across business functions, and used to set the parameters for the data governance strategy and the role data will play in solving business problems and executing on business goals. With that as the foundation, data governance leaders can begin establishing awareness and knowledge of the organization's data assets.

Core elements of building the program include:

1. **Know thy data!** Firms that do not have an accurate categorized and contextualized data inventory, or overlook data as a pillar of key activities, are literally operating from an information deficit. Whether it is data relating to products, customers, employees, inventory, partners, etc., lack of awareness will almost always result in competitive disadvantage and undervalue the asset class as a whole.
2. **Improve data quality:** Inaccurate or incomplete data can lead to poor decision-making, as well as legal and regulatory issues. Having a robust awareness of all data assets can help identify data quality issues and ensure that corrective actions are taken to improve accuracy and completeness.
3. **Business decision-making:** To make informed decisions, executives and managers need to understand the data assets available to them. This includes data on customers, competitors, markets and internal operations. Without this knowledge, decision makers may rely on incomplete or inaccurate information, which can lead to poor decisions that negatively impact the company's performance or fail to capture potential upside.

   An important sidebar about business decision making: As more firms embrace data and analytics and the illuminating results that come with it, knowledge of the firm's data assets and the quality of that data are crucial. As firms embrace data visualization technologies such as Tableau or PowerBI, or establish data science programs utilizing powerful data analytics technologies and programming languages such as "R," Minitab, Python, vector databases or others, the maxim used for decades (garbage in-garbage out) could not be more relevant. The better the data and it's quality, authenticity and reliability, the higher the yield from business decision making infrastructure. Data knowledge and quality are force multipliers for business decisions, particularly those make using data science and data and analytics.



4. **Information security:** Information security is a critical concern for organizations, especially considering the increasing incidence and risk of data breaches, data loss and cyber-attacks. A clear view of the internal data landscape will support identification of the data types (e.g. personal data, non-public information, intellectual property, confidential business records, etc.) and crown jewel locations that require extra protections and implementation of appropriate security measures.
5. **Legal, compliance and privacy.** In addition to complying with regulatory requirements to protect personal and sensitive data, firms that emphasize data compliance and privacy programs signal to the market that they are trustworthy stewards of personal and sensitive data assets. Robust data compliance and privacy programs can facilitate trust and enhance trusted relationships with customers, suppliers, employees and the public at large.
6. **Data stewardship:** Within any organization attempting to leverage data as an asset class there should be a group that has true ownership and responsibility for the asset. These stewards should remain separate from core IT operations. For example, if financial systems are maintained by the IT department, the actual accounting data is owned by the finance team. Similarly, other parts of the business should accept stewardship roles to understand data collection purposes, use and disposition opportunities as applicable to their functions.

Leaders from compliance, security and data stewardship functions are the foundation of a data governance triumvirate. These form the group that should be in place to plan, enable and functionally operate a data governance program.

Why do we have the data?

One of the most overlooked aspects of a corporate data governance program is the assignment of data stewards, which in some organizations are also the data owners. Far too often, companies without a data governance program attribute ownership of data to IT, when in fact the business that acquires, generates or uses the data should be treated as the owner. Depending on the size and sophistication of the organization, the role of data owner and data steward may be conflated.

Assigned data stewards and/or owners in an organization are the starting point for managing and maintaining data. They should be able to answer questions around why data is being collected, whether the data is needed and providing value, and if it be relied upon for business decisions. These stakeholders are also typically in the best position to identify increased value opportunities for data, including enrichment and monetization.

Some of the key obligations of data stewards include:

1. **Data quality:** Data stewards must ensure that data is accurate, complete, consistent and up to date. They are responsible for defining and enforcing data quality standards, monitoring data quality and resolving data quality issues.
2. **Data usage:** Data stewards must ensure that data is used appropriately and ethically. They are responsible for helping to inform data usage policies and procedures, monitoring data usage and enforcing data usage and retention policies.
3. **Data risks:** Data stewards must be aware of risks to data, including those of unauthorized access, lack of availability and regulatory risks such as privacy and data protection. They will have role-based access controls and maintain visibility into activity relating to the data under their purview.

For many organizations, the coordinator of the stewardship or data ownership roles is the **chief data officer**, **chief information governance officer** or other similar executive leader. That person has responsibilities including raising awareness of data stewardship responsibilities, providing training and support to data stewards, owners and users, and promoting a culture of data stewardship across the organization.

What must we do to protect the data?

Very deliberately in the diagram, there is a Venn-diagram appearance with overlaps in the three primary governance groups. There is an overlap between managing data as a strategic asset and complying with regulatory requirements related to data usage, privacy and data protection, security and confidentiality. This is the question as to “what” must be done with different

categories of data. The roles of **chief compliance officer**, **chief privacy officer**, and/or **chief risk officer** often have the remit for establishing what must be done to protect the data across an organization, which (as described in the next section) is often implemented by the IT teams under the supervision of the chief information security officer.

Although many organizations now focus on data privacy, overall data compliance involves identifying and adhering to legal and regulatory requirements related to the collection and acquisition, use, storage, transfer and sharing of data across a range of legal and regulatory obligations. This includes ensuring that applicable policies are communicated to data users and followed.

A comprehensive data governance program includes policies that require data to be classified according to its sensitivity level, with appropriate access controls in place, and which specify the period for which data be retained to comply with minimum and maximum retention periods. Data compliance requirements may also compel protection of sensitive data through encryption or other security measures.

However, once the policies define "what" will protect the data, the compliance organization must work with data stewards to ensure the policies are implemented and followed. In this way, these policies become business requirements that carry cross-department and cross-function responsibilities. Partnerships between the legal and compliance organizations and business units is essential to implementing comprehensive protection mechanisms to fulfill all requirements.

How do we protect the data?

Information security (infosec) is the technology leg of the data governance triumvirate as it aims to protect data against unauthorized access, use, disclosure, disruption, modification or destruction. The information security team has a key role to play in an organization's obligation to ensure that data maintains its confidentiality, integrity and availability (an easy-to-remember mnemonic: C.I.A.). The information security leader(s) is typically the **chief information security officer**, or **chief technology** or **chief information officer** in the firm.

The infosec team facilitates the implementation of security controls and requirements received from the data owners and the compliance team. For example, where a legal requirement to "encrypt the data" might be directed, the InfoSec team then implements encryption. In other words, data stewards and compliance team members do not necessarily have the technical knowledge of how to implement and manage access controls or data loss prevention programs, but they can direct them to be implemented in coordination with the infosec team.

As data is added or acquired, the infosec team will also support data cataloging and inventory technology, feeding information back to the owners and compliance teams for active due diligence, and using that as a basis to implement and improve data loss prevention programs.

A controls-based approach to data protection is a holistic method that provides measures, key risk indicators, key performance indicators and other metrics. These are an indication of a healthy and functioning data protection function in an organization. Part of the obligation from the infosec team back to the business and others should certainly be periodic metrics reporting about the security programs applied against the data and its attributes.

Hallmarks and benefits of data governance

When key leaders and their designees know the why, what and how with respect to the treatment of the data asset class, data governance can happen. Together, these leaders can implement a charter and policies with standards and guidelines, controls, monitoring, testing and metrics and structure these in such a way that the regulatory, risk and asset points of view are uniformly and strategically applied.

Key policies that should be in place with a strong data governance function may include:

- Privacy policy
- Information security policy
- Defensible disposition policy
- Data collection and fair use policy
- Information risk management portion of business continuity planning
- Data classification policy
- Data governance and data quality policies
- Information risk management and litigation hold policy
- Retention schedule

What is the value of the data?

Certainly, just to get to this point has been a journey! With that acknowledgement, once an organization knows its data and has a governance and oversight team in place, it can begin managing data as an asset class. To effectively treat data as an asset, financial teams should also be involved to ensure that the appropriate financial and accounting oversight of this asset class is in place. That may include and involve the fair valuation of the data, or accounting for activities associated with the enrichment, use and monetization of data.

Many organizations maintain a large amount of "goodwill" on the balance sheet. Understanding when some portion of value from goodwill relates to the value of the corporate data as an asset class of its own will help with maintaining the data so that the asset is managed and leveraged with the appropriate governance and controls in place over the long term.

Data valuation can take on two distinct dimensions:

1. What monetary value can be directly derived from the use of the data?
2. What intrinsic and/or enrichment value does the data add to corporate operations, such that if it were absent, other assets and/or operations would decrease in value?

In the first grouping, it is useful to think about new ways to use old data, or new data that could be collected within the bounds of the governance structure, and directly monetized.

The second grouping involves understanding what insights can be derived to drive more sales or revenue to existing lines. Is there or should there be a data science or data analytics team that is evaluating data to detect historical trends and patterns in the data or identifying opportunities for mass customization to drive customer or client adoption and delight? The practice of data analytics has become remarkably adroit with powerful tools for analysis and data visualization to reveal such insights.

Regarding the second grouping, many organizations fail to consider the negative consequences of the loss of their data via damage, malicious acts or neglect. Systems and processes, separate from data, constitute large aspects of the non-tangible assets of a firm, such that operations and stakeholder value would quickly diminish if the data underlying their systems and processes were to become unavailable. Additionally, enterprises can miss valuable commercial opportunities if the quality of data used for decision-making degrades over time, or if personnel spend otherwise productive time searching for appropriate information.

With a clear understanding of the value of data and engagement of the financial team, further benefits to both protecting data and monetizing data can be initiated.

Revenue generation and monetizing data

With a clear understanding of the notional content and value of the data of the enterprise along with governance in place to uphold the operational, ethical and regulatory requirements and obligations relating to and arising from the use of that data, organizations are empowered to make decisions about whether to implement steps to mature data operations into a revenue-generating capability.

Where monetization of data has perhaps been historically generalized as the sale of data, a direct quid pro quo as a data broker or a seller of data for marketing or other purposes, the definitions herein intend to apply more broadly. Monetization in this discussion includes revenue generation derived by corporate data to not only include direct sale or brokerage of data, but other methods in which firms increase their revenue directly via the enhanced use of the corporate data asset.

Through this lens, monetizing data for may include:

— Revenue driven by increased understanding of data and additional uses derived through machine learning.

— Revenue driven by use of corporate data via improved governance to drive AI and beneficial results.

— Revenue driven by the use of data for selling additional services (e.g., IoT data being used to sell supporting services).

— Other revenue that improved governance and valuation processes yield that are net-new and would otherwise not have been possible.

With the vast amounts of data organizations store, it can seem overwhelming to consider mining that data to identify current trends or opportunities. To date, online retailers appear to be among the furthest ahead on this, using data to identify when a customer or prospect needs a refill or to replace something that has limited quantity or depletion timing (e.g., refrigerator water filter). Other examples include using data for tracking of mean time to failure (MTTF) of certain components, as these can be predicted (dishwasher pumps, freezer compressors, batteries, etc.) and can be customer-facing to provide helpful notices and reminders.

In contemporary conversations, there are many misconceptions that the power of artificial intelligence can be realized without prerequisite work on the quality of the data and the model that is going to feed the AI or generative AI tool. Regardless of the type of AI (e.g., custom large language model (LLM) or applied tools such as GPT), each model is based on *data that must have the requisite quality, validity, reliability and variety* to produce helpful and accurate results, as well as meet usage requirements, including legal and compliance clearance. Starting down the path of AI implementation without a data governance program to facilitate those requirements (and defend and articulate the sources of the data) will be at best challenging, costly and potentially disastrous. Data governance is needed to drive confidence in and understanding of permittable uses of the firm data assets, ensure the model is fed quality data that can be used for intended purposes, and the results are tested, repeatable and accurate.

Conclusion

As board members, executives, and others make the push to enhance offerings and drive predictable sources of revenue, an organization that places data at the center will find that the approaches outlined here offer a roadmap to data monetization and success in pursuits from basic modeling to machine learning to generative AI.

Implementing and maturing Data Governance permits a company to step along the continuum from data awareness to deriving greater value indirectly and directly from data, including through data monetization. Many organizations attempt to take shortcuts and end up with results that can be of questionable quality and little value. If organizations start to think about their data as an asset class, and like any other asset, ensure it is maintained, protected and has the oversight and attention of corporate leaders of the firm, it can quickly become one of the higher performing, revenue yielding assets.

SCOTT MARGOLIS
Managing Director
+1 303 885 7728
scott.margolis@fticonsulting.com

DERA NEVIN
Managing Director
+1 917 499 7450
dera.nevin@fticonsulting.com