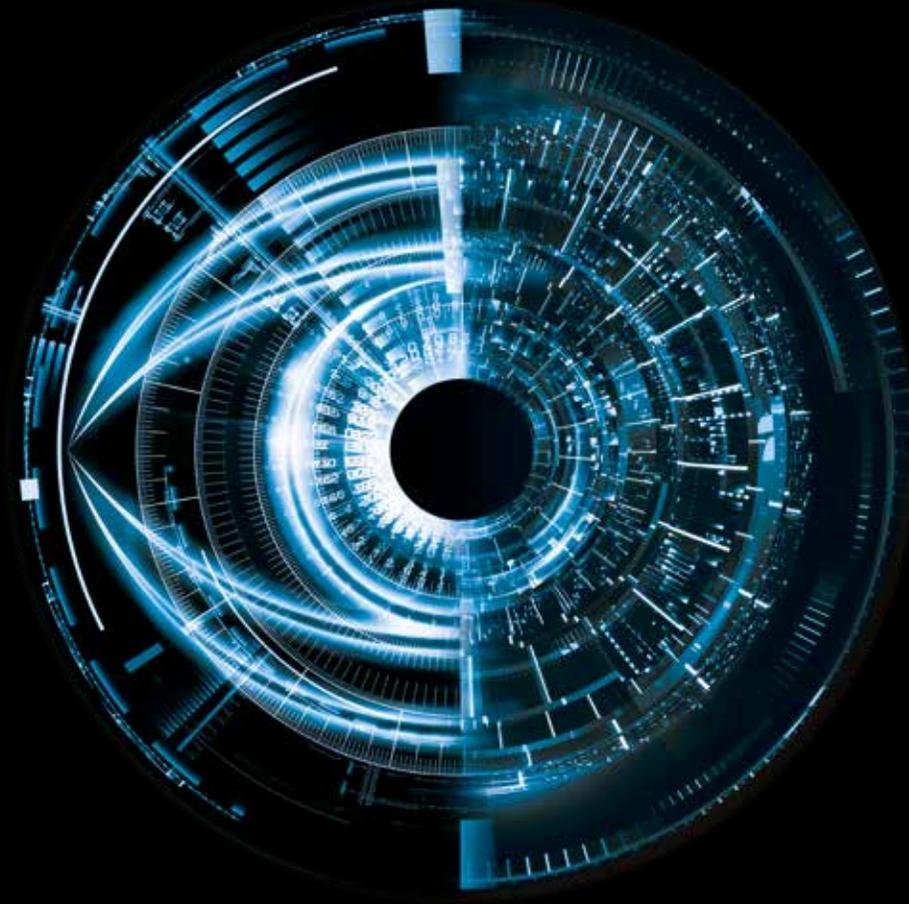


Deloitte.



**Treat your data like the superpower it is:
Making the case for data governance**



Data governance has always been important, and a changing risk and regulatory landscape is accelerating the need for a strong, strategic program.



No matter the industry, companies today possess massive amounts of data. Technology, media, and telecommunications (TMT) organizations collect, store, and manage data that ranges from personal identifiers to behaviors, from shopping preferences and internet searches to health and eating habits to call logs and location tracking. Perhaps unsurprisingly, increased customer concerns around privacy issues and constant media coverage around significant data breaches have generated more interest in governmental intervention, regulatory measures, and increased privacy protections.

The increased scrutiny and conversation around data privacy has led to regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

While GDPR originated in the European Union, the reality is that many TMT brands have a global digital footprint and are subject to these regulations. In the United States, it's likely that state-level governments will roll out their own versions

of CCPA and that federal regulations are on the horizon. Each regulation could have its own definition of personal or private data, its own set of specifications of individual rights associated with organizational data management, its own set of directives for compliance, and its own set of reporting and auditing requirements.

What does this mean for data from an organizational perspective? Compliance may include an ability to determine whether each data asset contains information covered under any number of regulations, the compliance rules to satisfy regulatory directives, the methods for validating and reporting on compliance, and a number of other possible requirements. When it comes to personal data protection, this creates a requirement for data asset classification, categorization, and documentation. As data breaches make headlines and ongoing privacy concerns drive regulatory measures, TMT executives are pushing comprehensive data governance to the front burner.



Why data governance is still in vogue

“The voice of the customer is driving many of these regulations. Companies should know their customer and put them first. They may be willing to share their data, but they need that transparency for a great, lasting customer experience.”

—Dan Sutter

The term governance can be cringeworthy for TMT leaders, even those that run the information and digital strategy. Successful TMT brands have thrived on agility, creativity, and accelerated speed to market—without significant regulatory hurdles. Digital transformation is driven through data, and data has evolved into a significant asset in highly competitive TMT markets with low barriers to entry.

Some TMT organizations have invested heavily in data infrastructure to host data assets, but with the speed of transformation, the systems may not have been implemented in an orderly fashion. Data lakes store and categorize the digital outflow, but organizations failed to apply controls to circumvent lakes from devolving into swamps. Simply put, data privacy is a driver behind much larger shifts that TMT leaders

need to get ahead of—and no organization can afford to wait. The stakes are particularly high in TMT given the vastness of data among multiple disconnected systems for collection, storage, and use.

While data governance is crucial to manage such an important asset, it hasn't always been a priority for TMT organizations that grow at a breakneck pace. Increased regulatory pressure is changing that, with GDPR and CCPA creating a newfound sense of urgency.

Many leaders across organizations are motivated to take a fresh look at modern data governance programs and make the case for strategic investment.



**Data integrity means
better decisions**



Governance can be beneficial from both business and operations standpoints. Identifying personal data and validating that data across ecosystems can help with compliance, and it can also help solve for other challenges such as data quality issues and unstructured data stores. Whether a TMT company survives or thrives has often been dictated by its ability to scale data-based business models; use the data to make business decisions; and underpin innovation in its products, services, and customer experiences.

Data is an asset and, like most organizational assets, actively managing it is an effective tool to extract maximum value. Too often, organizations find they don't know what data exists throughout their enterprise and how it's being used across business functions, geographies, and ecosystems. In addition to regulatory compliance, the growth of unstructured data and the difficulty in getting

data to the people who need it is another prominent driver for data governance to restore order. Data is being used to make business decisions on everything from budgets to new products or from partnership development to marketing. Data governance is an overarching strategy to validate that the data is clean, accurate, usable, and secure. TMT executives across the organization rely on data as a form of currency. As a result, data integrity and good governance are crucial in making real-time business decisions for the future of the organization.

Data is a shared asset, and the proliferation of users creates new allies to support investments in governance. Data stakeholders, such as business units, the compliance department, and IT, have traditionally been positioned to lead data governance. Digital transformation and the pivot toward data-driven organizational models have expanded governance stakeholders and created new allies within TMT organizational



hierarchies. Rising numbers of chief data officers are reporting to the chief executive, and the chief marketing officers and chief content officers are increasingly familiar with tools of governance, including metadata and data lineage.

To create a successful data governance program, organizations must align people, processes, and technologies to identify, classify, and document information about their data assets. Organizations can build collaboration among data owners and data consumers to eliminate any confusion over what data means or where it resides. By engaging employees from various departments and clearly defining roles and responsibilities, organizations create a consistent and concrete understanding of data across the enterprise to empower business decisions, while also effectively navigating complex regulatory mandates.

Trust and the customer experience are value drivers rooted in strong data governance. Deloitte research has shown that if customers are given control over their data, they're more comfortable sharing it. For companies with business models that rely on customer data, providing transparency can go a long way. The first step to provide that level of transparency requires a data governance program that accurately reports what data a company has, how it is using it, and where it is stored or shared.

However, this transparency comes with some risk. More self-service interactions with customers means collecting and packaging more information about customers, accounts, purchases, and preferences. More data can lead to a better customer experience, but it can also increase risk of exposure of personal or confidential information. Now,

couple that security challenge with the regulatory and legal restrictions that companies must adhere to under privacy regulations. From the 2018 deadlines for GDPR to the upcoming CCPA laws, these regulation-specific responses are complex, and companies can face penalties if they fail to achieve compliance.

Solid data governance processes are relevant to an organizational executive concerned with meeting GDPR, CCPA, and other regulations. For example, the process of data lineage helps an executive understand the data life cycle. The data lineage process chronicles the flow of data through an organization from its origin points, generally beginning with a customer or through its use and consumption at varying stages. This life cycle process illustrates the points where data is accessed, used, reported, changed, or used to derive new data.

Third party companies are subject to the same data privacy and security standards as the organizations they serve. The data privacy and regulatory landscape is such that companies are now reviewing contracts to ensure that third parties that have access to their data—or data they've monetized—are held to the same privacy and security standards, and they are doing so by appropriately amending contracts. In a matter of minutes, an organization should be prepared to respond to a breach, even if it occurred with a third party. Having a clear understanding of where data is and how it's being used across the ecosystem helps TMT organizations proactively maintain awareness of vulnerabilities and threats.





**The best defense is a
good offense**

“Data is your new currency. So data integrity is crucial because it helps you make reliable and targeted business decisions around the future of the organization.”

—Richard Vestuto

With regulations and reputational concerns pushing compliance leaders to the top levels of management, TMT organizations should begin by taking stock of where they are and where they need to go, keeping the current landscape and regulations at the forefront of data strategy. Data governance is about not only maximizing the value of data for operational effectiveness, decision-making, and regulatory

requirements, but also minimizing the risks associated with poor data management. Data privacy considerations should be embedded in every step and include stakeholders across functions, from IT and operations to marketing and sales. Good data governance involves various steps and a well-defined framework.





**How can TMT organizations
get there?**

Gain acceptance across the organization of shared ownership.

Data is not owned by just one function, rather it is the responsibility of the entire organization. While data governance requires buy-in from the top down, it's critical that everyone who handles or uses data is involved in the process. This way, the governance structure reflects the way the organization operates—and where it's going.

- **Who will represent each function across the organization?**
- **What roles and responsibilities do we need to clarify?**
- **What are the points of accountability?**

Decide where the organization is going.

Organizations should think beyond the current regulatory requirements of GDPR and CCPA. We suggest taking a comprehensive view of regulatory requirements. In other words, consider compliance an ongoing journey. TMT organizations should think about long-term business strategy as well. Doing so helps readdress or reprioritize where to focus attention, such as identifying certain systems or data fields that need attention.

- **What is the long-term goal for data strategy and governance beyond compliance?**
- **What is the brand's current global footprint? Where might operations expand in the future?**
- **How much governance is needed along each milestone of the data life cycle?**

Take stock of the current position.

Before blazing ahead, organizations should assess where they are from policy, governance, resources, risk, and operational standpoints as well as consider the guiding principles they will use to support a privacy-related strategy. If customer data is the most valuable asset for the organization, that should be their North Star. Once an organization has identified these areas, it can assess what measures are already in place, what needs to be updated, and where to start fresh.

- **Where is data the most vulnerable?**
- **What data governance approaches exist and what tools are organizations using?**
- **How do the guiding principles need to be modernized going forward?**

Conduct benchmarking and market analyses.

These activities can help TMT organizations understand the risk landscape as well as how prepared they are as an organization. TMT organizations may find that benchmarking against competitors is only one piece of the puzzle and looking at other industries can provide a clearer picture of the markets in which they operate. For example, online retail organizations may benchmark against select brick-and-mortar retailers.

- **What capabilities are organizations building for data governance?**
- **What customer experience benchmarks do we need to think about?**
- **How is this market intelligence going to inform our data governance strategy?**



TMT organizations will continue to see the data privacy and the regulatory environment expand in the coming years. To keep pace with the demands of the marketplace and customers, TMT organizations need to reframe their approach to data governance and identify the value it will deliver to the organization. Burgeoning compliance obligations and heightened expectations around transparency have increased operational challenges while stricter regulatory enforcement efforts and relentless public scrutiny have magnified potential business impact.

These same trends have amplified the challenges and have also made compliance a board-level concern.

By organizing and operationalizing the treatment and management of data, TMT organizations are positioning themselves to manage current compliance requirements and effectively respond to new ones. By taking the steps to ingrain data governance in the DNA of the organization and dust off outdated policies, TMT organizations can overcome these obstacles and make more informed business decisions now and in the future.



Contact Us

Jana Arbanas

US Telecommunications, Media & Entertainment Lead
Principal | Deloitte Risk and Financial Advisory
jarbanas@deloitte.com

Christina DeJong

Partner | Deloitte Risk and Financial Advisory
christinadejong@deloitte.com

Glenn Aga

US Cyber Risk Services
Managing Director | Deloitte Risk and Financial Advisory
glennaga@deloitte.com

Daniel (Dan) Sutter

US Cyber Risk Services
Senior Manager | Deloitte Risk and Financial Advisory
dasutter@deloitte.com



This document contains general information only and Deloitte Risk and Financial Advisory is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte Risk and Financial Advisory shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, "Deloitte Risk and Financial Advisory" means Deloitte & Touche LLP, which provides audit and risk advisory services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.