TONE at the TOP®

Providing senior management, boards of directors, and audit committees with concise information on governance-related topics.

Issue 97 | February 2020

Data Governance: What Directors Need to Know Now

A sea change is taking place in corporate governance, and it's all about data.

Director responsibilities are constantly evolving, but once in a while, there's a dramatic shift: a time when the rules of sound governance are fundamentally transformed. It happened shortly after the fall of Enron Corporation, for example, when waves of governance failures led to enactment of legislation such as the Sarbanes-Oxley Act. Almost overnight, director responsibilities changed significantly. Board agendas expanded to previously unimagined complexity, and meeting schedules multiplied.

Another corporate governance upheaval is taking place today. This time, it's not about financial controls; it's about data. And it might be the biggest governance change yet.

It's no wonder that board responsibilities regarding data are changing. According to a 2018 article at Forbes.com, an incredible 90 percent of the world's data was generated during the previous two years. Every day, the world produces more than 2.5 quintillion bytes of data, and the pace is still accelerating. Some analysts estimate that while today's data centers consume about two percent of the world's electricity, that figure will reach eight percent by 2030.

What's more, the advent of 5G wireless technology promises to increase data collection *exponentially*. Where current discussions about data collection involve gigabytes (billions of bytes), the new technology will enable data collection in zettabytes (trillions of gigabytes). This long-awaited tech revolution will empower organizations to collect massive amounts of data to inform strategic business decisions and integrate intelligent data into everything.

New Opportunities Bring New Risks

With so much information residing within corporate systems, data governance processes have a critical impact on operations, compliance risks, and the bottom line. Data and analytics have the potential to affect our organizations far beyond the scope of information security and technology. They are

About The IIA

The Institute of Internal Auditors Inc. (IIA) is a global professional association with more than 200,000 members in more than 170 countries and territories. The IIA serves as the internal audit profession's chief advocate, international standard-setter, and principal researcher and educator.

The IIA

1035 Greenwood Blvd.
Suite 149
Lake Mary, FL 32746 USA

Complimentary Subscriptions

Visit www.theiia.org/tone to sign up for your complimentary subscription.

Reader Feedback

Send questions/comments to tone@theiia.org.

Content Advisory Council

With decades of senior management and corporate board experience, the following esteemed professionals provide direction on this publication's content:

Martin M. Coyne II
Michele J. Hooper
Kenton J. Sicchitano

bringing dramatic new options to the business world, including new forms of marketing, manufacturing, research, and work. Some of those new options come with hefty revenue streams.

Take the automobile industry, for example. Today's connected cars use sensors to generate data about internal status and processes and to gather information about road conditions, traffic, weather, and even who's behind the wheel. That data has significant economic value. Car manufacturers apply the data in product design, marketing, quality initiatives, and recall management. They can use it to steer customers toward recommended maintenance and repair. But information from connected cars can also be sold to insurance companies and other third parties. A report from McKinsey & Company estimates that by 2030, annual global revenue from car data monetization might reach $750 billion. And in the event of an accident, emergency messages from data-connected cars can even save lives. (The European Parliament has created an eCall requirement for new cars specifically for this purpose.)

Big data comes with big opportunities, but it also comes with big new responsibilities. Collection of that automotive data means companies will have to be able to prove that customer consent was given and validly obtained. Data ethics, privacy, and transparency must be considered throughout the development and delivery of new products and services. Safety concerns necessitate data accuracy, and data breaches must be disclosed in accordance with rules that vary throughout the world.

In the United States alone, there are numerous federal and state laws and regulations regarding data protection, with multiple regulatory authorities responsible for oversight. The requirements are constantly changing: For example, the California Consumer Privacy Act (CCPA) just went into effect in January, and lawmakers are already proposing changes. Dozens of other states have introduced bills related to data privacy, and Congress is considering substantial reforms to federal data privacy laws. According to the Information Technology & Innovation Foundation, if the proposed

federal legislation mirrors key provisions of either the California rules or the Global Data Protection Regulation that went into effect in the EU in 2018, then the new requirements would cost the U.S. economy approximately $122 billion per year. That comes to about $483 per U.S. adult just for compliance with privacy laws.

The costs of compliance are staggering, but compliance with privacy regulations is merely a single issue within data governance. Governance programs also consider issues such as data integrity, accuracy, completeness, consistency, efficiency, effectiveness, confidentiality, availability, reliability, and ethics. That's a big job, and it's getting bigger every day.

Director Liability

There's a growing risk of personal liability for directors who ignore data privacy rules or other essential governance requirements. In June 2019, the Delaware Supreme Court issued a decision reaffirming director liability where there is no board-level reporting process for essential compliance matters. In Marchand v. Barnhill (the "Blue Bell decision"), the court stated that it is an act of bad faith of the duty of loyalty when directors fail to attempt to assure that a reasonable information and reporting system exists. Although directors and officers generally are immune from liability, in most states directors cannot be "absent from the fundamental matters" of the corporation. Directors also fail in their duty of oversight if they consciously fail to "monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."

While the decision in the Marchand case, which continues to work its way through the Delaware courts, focused on the board's failure to oversee "mission critical" risks involving food safety, the upshot for boards is, what you don't know can hurt you.

DATA GOVERNANCE QUESTIONS FOR DIRECTORS

1. **What data are we concerned with?**
   Effective data governance starts by knowing what data is being collected, where it resides, and how it's being used throughout the organization. In many cases, mapping the flow of data can enhance understanding and strengthen data governance.

2. **Is our data being used properly?**
   The data governance system should help assure that data is available when needed for legitimate business reasons, but it must also protect sensitive information and assure that data is used ethically. Directors need to know whether or not the company has created adequate policies and procedures on data usage, and they need to ensure that there are controls to monitor and enforce the policies.

3. **Have we defined specific goals for our data governance program?**
   Every company is different, so there is no standard one-size-fits-all approach to data governance. If the data governance program is relatively new, for example, it might be a considerable undertaking merely to determine where all of the organization's critical or sensitive data resides. Later, the focus might shift to minimizing risks, increasing the value of data, improving the flow of information, or other priorities. Therefore, data governance goals and priorities should be reassessed regularly.

4. **How have we evaluated the risks?**
   Every company has to deal with risks such as data loss or corruption, data breaches, or compliance lapses. It's impossible to eliminate all risk, but it's important that the board receives timely information about significant data risks and evaluates whether or not the level of risk exposure is appropriate for the company's risk appetite.

5. **When significant issues are identified, how do we assure that they are handled appropriately?**
   The board needs to understand the processes for communicating and addressing significant data governance issues. They also need to ensure that when problems are identified, they are addressed appropriately.

6. **What about data governance frameworks?**
   A data governance framework provides guidelines for using data, managing it, and resolving data issues. It identifies the people and departments that should control and manage different types of data. Organizationally, the framework might include a data governance office that helps run the program, along with a data governance committee or council that prioritizes data governance projects; approves data usage policies, processes, and procedures; and identifies data stewards and stakeholders. If your company has not yet agreed upon a data governance framework that assigns specific responsibilities, it may be time to ask why not.

   Resources:
   NIST Cybersecurity Framework
   NIST Privacy Framework

Board Responsibilities

A decade ago, data governance might or might not have been a topic on the board's agenda. When data was included on the agenda, the discussion was often limited to a single aspect of data governance, such as information security or data privacy. And if directors had questions about data governance, they often simply relied on management to give them the information they needed.

Given today's data risks, that approach is no longer adequate. In a recent report by Compliance Week, 46 percent of surveyed boards were briefed at least quarterly on data governance. Almost half had implemented or updated internal privacy policies, and 43 percent had expanded data privacy resources and budgeting in the past year. Only five percent of survey participants were not briefed about data governance at all.

To fulfill their duty of oversight, directors need independent, objective assurance that data risks are being handled appropriately. That means significant data governance risks must be audited. But directors also need to ask hard questions about data governance. According to *Governance in the Digital Age, A Guide for the Modern Corporate Board Director* by Brian Stafford and Dottie Schindlinger, "Boards need to know what they don't know, which requires a lot of courage. Directors need to be able to ask questions and be honest about what they don't understand, or they won't be able to provide the level of oversight and insight required today."

Quick Poll Question

Does your organization have a formal data governance program?

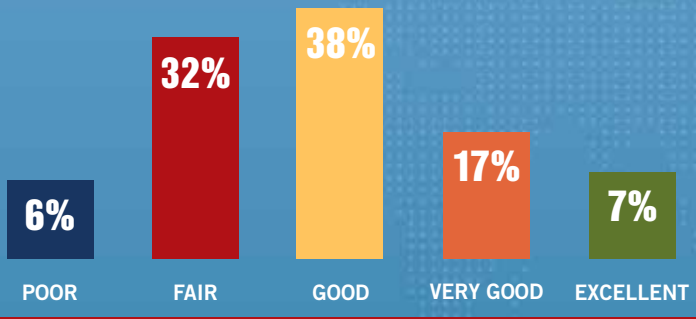
- ❑ No, and we have no plans to start one.
- ❑ No, but we are planning to start one.
- ❑ Yes, we have a program, but it is not mature.
- ❑ Yes, we have a mature* program.
- ❑ I don't know. It's time to find out.

Visit www.theiia.org/tone to answer the question and learn how others are responding.

** A mature data governance program assigns specific responsibilities, monitors compliance, and reports information regarding data governance to management and the board of directors.*

QUICK POLL RESULTS:

How would you rate the effectiveness of corporate governance leadership by your board and management?



Source: Tone at the Top December 2019 survey.