

Data risk management

Our point of view

November 2024

Contents

Introduction	1
Data risk management: An industry perspective	1
Trends in managing data risk across financial services	1
What are financial institutions doing to manage data risk?	3
What challenges may impede companies from managing data risks?	4
Our point of view	5
Managing data risks: Key tenets	5
Managing data risks: Recommended actions	6
How can we help?	10
Deloitte assets to accelerate data risk management	11
Contact us	12

Introduction

Managing data risk is a crucial challenge for financial services organizations, as they face increasing regulatory scrutiny, customer expectations, and competitive pressures. Data risk can affect not only the security and privacy of sensitive information, but also the quality, accuracy, and availability of data that supports business processes, decisions, and outcomes. In this article, we explore some of the key trends and challenges in data risk management across the industry, and how organizations can leverage leading practices and tools to address them.

Data risk management: An industry perspective

Trends in managing data risk across financial services

In recent years, a variety of trends related to data risk have significantly influenced financial services organizations worldwide. These developments stem from external influences, such as evolving regulatory requirements and expectations, as well as internal shifts toward a more data-driven approach to decision-making and the adoption of emerging technologies such as artificial intelligence (AI) and machine learning (ML). Four of the more prominent trends are described below.

Regulators are becoming more data savvy and continue to actively monitor data

Recent advancements in data literacy among regulatory agencies have notably raised the bar for compliance expectations. Regulators are now demanding data that is better organized, more granular, traceable, and collected more frequently. Organizations that fail to meet these heightened standards face significant penalties, as shown in figure 1.

Figure 1: Regulatory actions




2024			2023	
Enforcement action against top US bank for lack of data integrity, data lineage, documentation, and controls	Wealth management organization fined \$348M for data gaps in trading surveillance and data reconciliations	Top US bank fined \$135M for insufficient progress on data quality management and failure to implement controls to manage ongoing risk	Top US bank fined \$186M for lack of data tracing, data integrity, data management program, and data Governance	Top US bank fined \$12M for lack of data accuracy, data collection, and false mortgage data

Leadership and consumers expect increased levels of confidence in data

As organizations have come to rely more and more on data to drive decision-making, leadership and consumers have come to both expect and rely on data that is of high quality and ready for use. Traditionally, organizations have largely focused on a set of core data risks, but this is no longer sufficient to ease concerns around data. In today's digital landscape, it is paramount to also identify and mitigate emerging data risks to provide the level of confidence in data that leadership and consumers demand.



Figure 2: Core and emerging data risks

Confidence in data comes from managing core data risks...

-  **Data quality risk** (e.g., inaccurate/inconsistent data)
-  **Regulatory compliance risk** (e.g., misinterpretation of regulations)
-  **Data privacy risk** (e.g., storing large volumes of Personally Identifiable Information (PII))

+

...while identifying and mitigating emerging data risks such as –

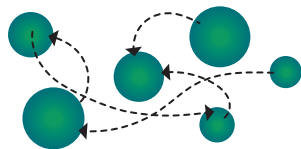
-  **Emerging tech risks** (e.g., application of Artificial Intelligence (AI)/Machine Learning (ML))
-  **Third-party risk** (e.g., data ingestion/distribution)
-  **Unstructured data risk** (e.g., inadequate data inventory)

More structured and formalized approach to data risk management

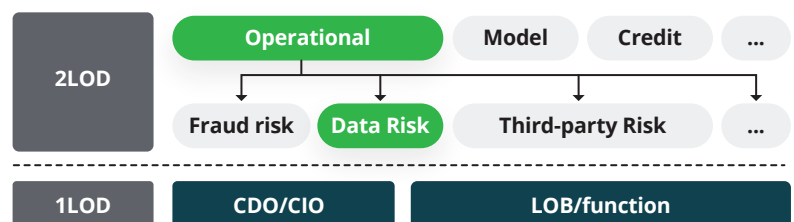
Financial services organizations are inherently complex, navigating a landscape marked by regulatory requirements, diverse product offerings, and complex operational structures. Consequently, such organizations must manage a broad range of risks, such as market, credit, compliance, and operational. Given these competing priorities, data risk often takes a back seat and is managed sporadically or inconsistently across organizations. But as mentioned above, both external and internal factors are forcing organizations to prioritize data risk and formally establish it as a risk stripe within their enterprise risk framework.

Figure 3: Structured data risk management

From reactive and ad-hoc management of data risks...



...to formalizing the data risk stripe and function



Board and management visibility into data health and data risks

The success of organizations is exceedingly becoming dependent on their data as they move toward becoming more digital, data-driven, and reliant on data to make informed decisions and drive their business strategies. Data is an increasingly valuable and risky asset that is critical to the success of the business. These trends are pushing boards of directors and management teams to measure and understand the health of their data to drive better accountability and outcomes through enhanced reporting (i.e., visibility) into data risk starting with targeted focus areas:

- **Executive views:** Inform decision-making and provide high-level insights.
- **Business views:** Provide business-specific insights and drive accountability.
- **Operational views:** Manage progress and monitor operational effectiveness.
- **Custom views:** Enable users to “slice and dice” information for custom uses.

What are financial institutions doing to manage data risk?

Data risk is a complex and evolving challenge that requires a coordinated and proactive approach from all stakeholders. Financial institutions are recognizing the need to embed data risk management into their overall governance, risk, and compliance frameworks. To achieve this, they are pursuing a range of initiatives that aim to improve their data quality and data governance, as well as to enhance their data capabilities and culture. Organizations are taking some of the following key actions to manage data risk:

- Establish a **shared agenda across the three lines of defense** to holistically identify and manage data risks
- Establish **policies and standards for data risk identification, management, and accountability**
- **Standardize data risk definition, taxonomy, and metrics and reporting** to enable prioritization of risks and monitoring
- **Drive education and awareness of data risks** through standardized change management and communications
- **Embed data risk issue criticality and escalation criteria** into enterprise issue management processes
- **Aggregate, report, and monitor data risks** consistently across the enterprise

What challenges may impede companies from managing data risks?

One of the key steps to effectively managing data risk is to identify and prioritize the sources and drivers of data risk across the organization. However, many organizations face significant barriers in this process, preventing them from developing a comprehensive and consistent view of data risk and its impact on their strategic objectives and operational performance. Below are eight common challenges that organizations need to address to overcome these barriers and manage data risk effectively:

1

Lack of accountability or **formalization of data risk** within the enterprise risk framework

2

Lack of clarity in ownership of data risks between data management, data privacy, and information security

3

Limited understanding of data risks and their impact within the first line of defense

4

Challenges **educating the enterprise** and communicating the importance of data risk management

5

Resistance to change and **“taking on additional responsibilities”** by incorporating data risk management-related activities into day-to-day business processes

6

Narrow concept of data risk that **focuses on managing known data risks** (e.g., data quality risk, data privacy risk) **but not emerging data risks** (e.g., application of AI/ML, third-party risk)

7

Data risks are **not holistically considered** and **are limited to data quality issues**

8

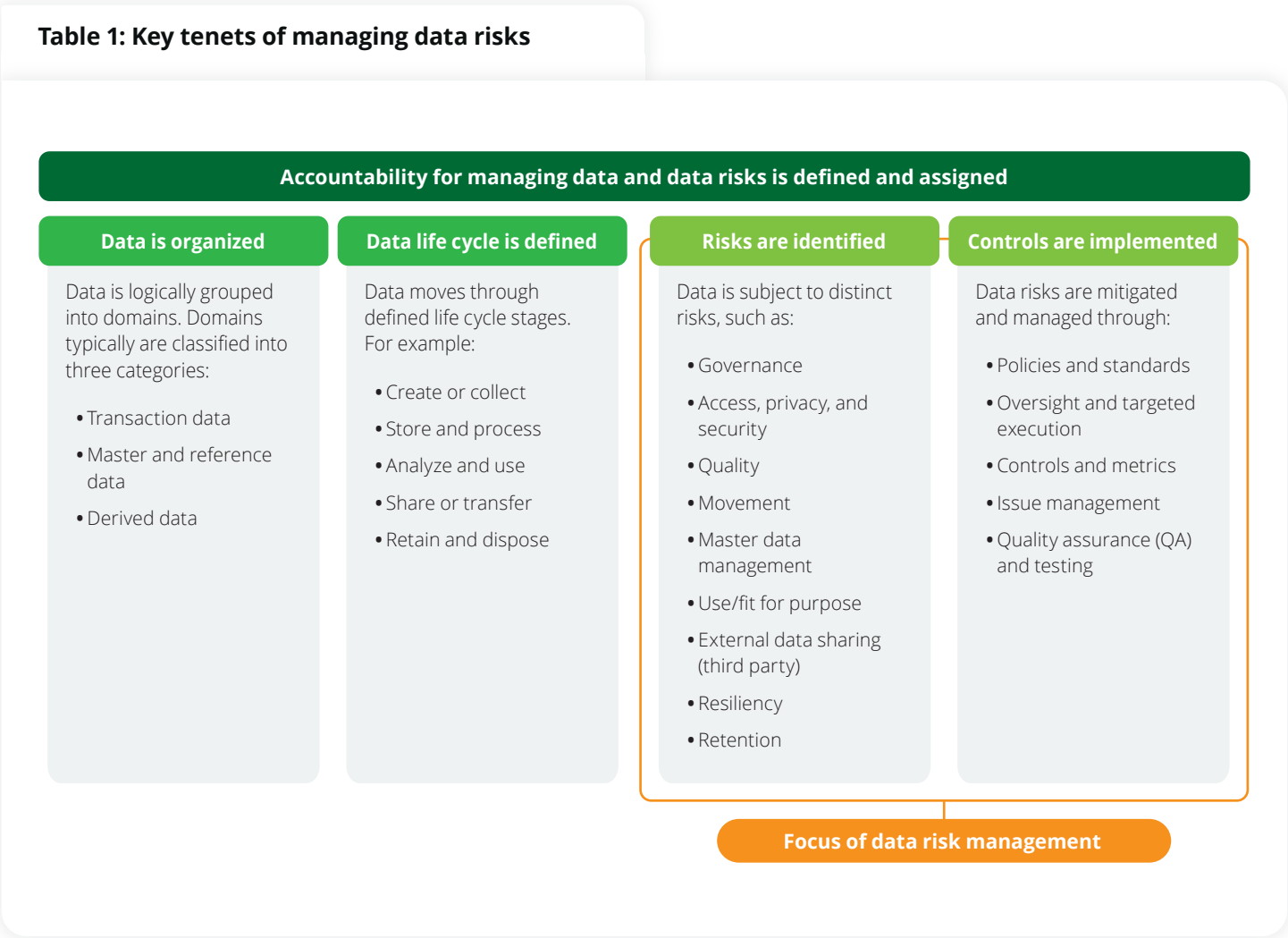
Limited visibility into the adverse impact of data risks across the enterprise

Our point of view

Managing data risks: Key tenets

Executing a data management program is a continuous process that requires coordination and alignment across the organization. Organizations focused on managing their data assets typically execute a data management program that addresses the following tenets:

Table 1: Key tenets of managing data risks



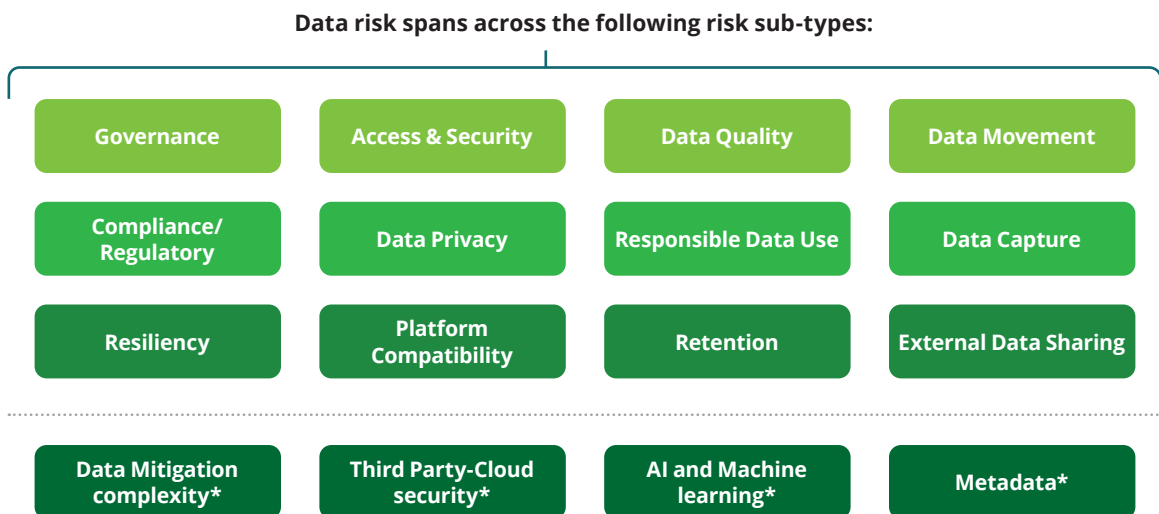
Managing data risks: Recommended actions

To begin addressing the key data risk management tenets mentioned above, organizations may take the following foundational actions:

Action 1: Define data risk

This includes defining applicable data risk sub-types, and developing the data risk taxonomy that can be followed by the organization. The definition of data risk may be tweaked and tailored to meet the business needs of an individual organization, but Deloitte often defines data risk as “the risk that enterprise frameworks, policies, standards, target operating models, and scope of coverage are insufficient to **holistically manage the organization’s data & metadata across its lifecycle**. It includes the risk **of failure in the collection, storage and retention, use, transfer, management, protection, and/or disposal of data that is captured, created, or acquired by an organization.**”

Figure 4: Data risk subtypes



*Emerging data risks

Action 2: Establish a robust data risk management framework

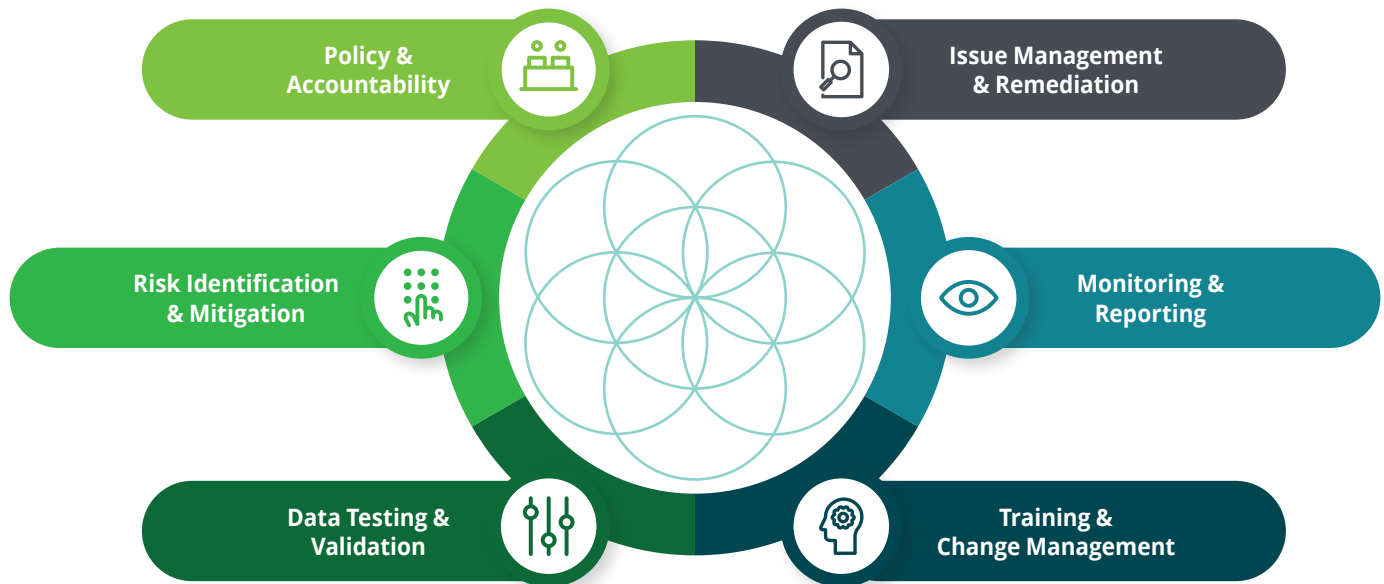
A robust data risk management (DRM) framework may enable organizations to establish a consistent and effective approach to identify and mitigate data risks, in alignment with enterprise data strategy. The framework:

- Empowers organizations to proactively **address risks associated with their valuable data** assets, through systematic identification, assessment, mitigation, and ongoing monitoring;
- Is **driven by several regulatory/business needs**, including regulatory scrutiny (e.g., compliance with regulations like GDPR), business needs (e.g., protecting sensitive data), and the evolving threat landscape (e.g., evolving data risks such as breaches, data readiness for AI use); and
- Typically is **enabled by a combination of policies/procedures, technology, and key personnel**. It includes governance and leadership, risk assessment methodology, data controls, incident response plans, and continuous monitoring and improvement.


Figure 5: Data risk management framework



Data Risk Management Framework



The framework consists of six key components:

1.  **Policy and accountability:** Define and implement policies, procedures, and standards to effectively manage data assets throughout their lifecycle and establish clear roles & responsibilities.
2.  **Risk identification and mitigation:** Identify data risks and establish risk response strategies related to acceptance, avoidance, reduction, or sharing of data risk.
3.  **Data testing and validation:** Perform testing of DRM activities to ensure effective risk identification, assessment, and mitigation.
4.  **Issue management and remediation:** Detect, assess, remediate, and escalate data issues as needed with the goal of limiting systemic and recurring issues and correspondingly data risks.
5.  **Monitoring and reporting:** Evaluate risk mitigation effectiveness through measurement of data risk exposure, and report on trends and emerging data risks.
6.  **Training and change management:** Enhance the enterprise wide data risk culture through implementation of robust change management and improved data literacy around DRM requirements, processes, and artifacts.

Action 3: Enable data risk management as a shared responsibility across all lines of defense (LODs)

Data risk management is a collective responsibility at every level, anchored in clear roles and responsibilities across the three lines of defense (LODs) of the organization.

Table 2: A shared responsibility

	First line (1LOD)	Second line (2LOD)	Third line (3LOD)
Policy and accountability	<ul style="list-style-type: none"> Ensure timely and trusted data availability while conforming to data-related policies and standards Create processes to standardize data risk management as a part of day-to-day operations 	<ul style="list-style-type: none"> Develop and enforce data-related policies and procedures Manage regulatory requirements related to data risk management 	<ul style="list-style-type: none"> Conduct independent assessment and audit to evaluate the effectiveness of data risk Policies, Standards, and Procedures (PSPs) Escalate significant deviations or instances of non-compliance
Risk identification and mitigation	<ul style="list-style-type: none"> Identify data risk associated with day-to-day business activities/processes based on system created by 2LOD Design and implement data controls across the life cycle Conduct self-assessments to evidence controls adherence 	<ul style="list-style-type: none"> Create a system for identifying, categorizing, and addressing potential data risks Prioritize risks based on likelihood and impact, and develop monitoring strategies to identify such risks Develop data risk-sharing strategies across LOBs 	<ul style="list-style-type: none"> Conduct independent assessment risk identification, assessment, and mitigation procedures and effectiveness
Data testing and validation	<ul style="list-style-type: none"> Document 1LOD data controls testing results, including identified issues or control deficiencies Take corrective actions by implementing new controls or enhancing existing ones 	<ul style="list-style-type: none"> Perform independent validation of 1LOD control testing results to test control design and performance effectiveness Provide recommendations to improve design and performance effectiveness 	<ul style="list-style-type: none"> Conduct independent assessment of data control design and performance effectiveness Report control deficiencies, weaknesses, or areas of non-compliance
Issue management and remediation	<ul style="list-style-type: none"> Identify, log, prioritize, and resolve issues related to data risk Perform root cause analysis and impact assessment 	<ul style="list-style-type: none"> Assess the effectiveness of issue management procedures and response plans Establish escalation channels for at-risk issues 	<ul style="list-style-type: none"> Conduct independent assessment of the organization's issue management processes to evaluate its effectiveness and identify gaps
Monitoring and reporting	<ul style="list-style-type: none"> Develop a data risk metric library and document calculation logic Monitor key data risk metrics and report anomalies or unusual activities detected 	<ul style="list-style-type: none"> Establish warning and breach thresholds for metrics Review, challenge, and oversee data risk metrics Develop data risk metrics reporting framework outlining scope, purpose, frequency, format, audience, etc. 	<ul style="list-style-type: none"> Regularly audit current data risk monitoring and reporting practices including data risk metrics and associated thresholds
Training and change management	<ul style="list-style-type: none"> Implement changes to data PSPs, processes, roles and responsibilities, reg. report, technology, etc. Ensure understanding of individual roles and responsibilities Design learning programs and champion data risk culture 	<ul style="list-style-type: none"> Foster a strong data risk culture across the enterprise Verify effective integration of implemented changes into DRM practices 	<ul style="list-style-type: none"> Review and test effectiveness of enterprise training Conduct 3LOD independent review, and test the effectiveness of the change management process Monitor the progress of change implementations

How can we help?

We can leverage our experience and assets to help prioritize and accelerate data risk management initiatives through a data risk management program or across specific components of the data risk management framework.

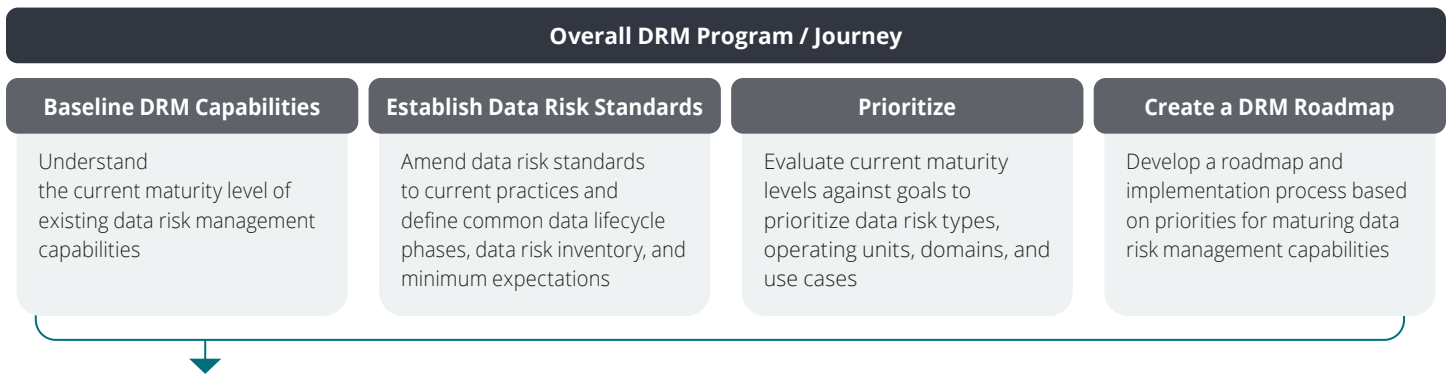








Table 3: How can we help?

Assistance across key DRM framework components		
	Policy & Accountability	• Create a Data Risk Policy and a Data Risk Operating Model standardizing data-related roles and requirements within the organization
	Risk Identification & Mitigation	<ul style="list-style-type: none"> • Define a Data Risk Taxonomy through risk assessments, prioritizing prevalent data risks and creating a system to identify, categorize, and address data risks in the future • Design data risk controls to test the effectiveness of data risk mitigation efforts and assessments to evidence controls adherence
	Data Testing & Validation	• Assess the effectiveness of risk identification, assessment, and mitigation efforts through data testing routines
	Issue Management & Remediation	• Identify and address data risk issues through issue classification and remediation escalation procedures
	Monitoring & Reporting	• Assist with ongoing compliance and risk oversight with data risk metrics and reporting routines
	Training & Change Management	• Build a secure data culture through e-learning modules and workshops and effective change management processes

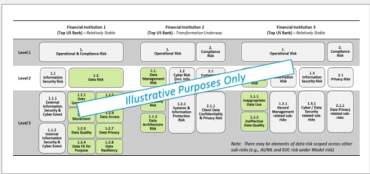
Deloitte assets to accelerate data risk management

Deloitte has a wealth of experience to draw on in this space, having worked with clients across industries and geographies to design and implement effective data risk management programs. We have developed several assets and accelerators that can help our clients achieve their data risk objectives faster and more efficiently. Whether you need to establish a data risk management program from scratch, enhance an existing one, or address specific data risk issues, Deloitte can help you navigate the complexities and deliver value from your data.

Table 4: Accelerators

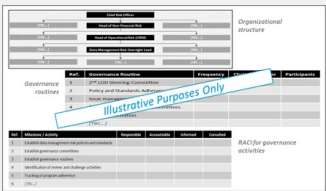
Data Risk Taxonomy

Illustrative examples of data risk taxonomies to assist with the identification, organization, and management of various types of risks associated with data



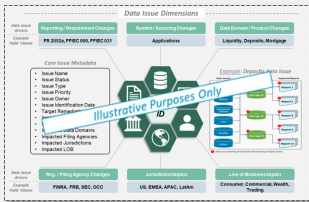
Data Risk Management Operating Model

Illustrative examples of data risk operating models focused on addressing the data risk management objectives and mandate of the organization and promoting a culture of effective data risk management



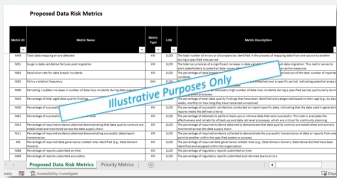
Issue Management Framework

Issue management framework that treats issues as multi-dimensional objects where required metadata is captured and the approach to prioritize and remediate issues is based on business objectives



Data Risk Metrics Library

Inventory of data risk metrics measuring data risk management performance organized by data risk sub-type, and with various attributes including metric owners, calculations, data required, data lifecycle phases, data risk types, and data sources



Contact us



Cory Liepold

Principal

Deloitte & Touche LLP

cliepold@deloitte.com



Satish Iyengar

Managing Director

Deloitte & Touche LLP

siyengar@deloitte.com



Ajay Ravikumar

Senior Manager

Deloitte & Touche LLP

ajr@deloitte.com



Chris Crow

Manager

Deloitte & Touche LLP

ccrow@deloitte.com

Contributors

Nikita Jain, Specialist Master, Deloitte & Touche LLP

Tyler Buresh, Senior Consultant, Deloitte & Touche LLP



About Deloitte

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication 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 adviser.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary 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.

Copyright © 2024 Deloitte Development LLC. All rights reserved.