TIMI OLAOYE
Monday October 9th, 2023

DATA IMPACT ASSESSMENT:
Understanding Data Risk from A Data Governance Perspective

Introduction

Data - "Where there is data smoke, there is business fire," a data enthusiast once said.

When organizations fail to create an environment whereby the value of data is not recognized, managed, and leveraged, it is usually a symptom of a much larger issue regarding how the organization is being run. Organizations that fail to prioritize data

nowadays are unwittingly not taking advantage of the innovation and numerous opportunities data has to offer - The competitive edge. Organizations not putting data at the center of their operational and strategic goals will fail to grow. In this article, we will introduce the Data Impact Assessment concept and its pivotal role in helping organizations discern and control data-related risks.

Data Impact Assessment (DIA)

Data is a powerful tool - Powerful tools require effective control and management to use it best. In essence, a Data Impact Assessment (DIA) seeks to systematically identify, evaluate, manage, and monitor the use of data before or throughout the lifecycle of a business initiative or project. A DIA identifies data risks that may arise and aims to bolster organizational capabilities on data risk mitigation. A DIA promotes conversations around data risks amongst all project stakeholders. Data quality, metadata management, data movement, adherence to regulatory and privacy obligations, and a host of data governance requirements are discussed in the DIA review.

Benefits of A Data Impact Assessment

1. Proactive Risk Identification

Proactivity from the standpoint of a DIA ensures that the smoke is detected and quelled before the fire expands beyond containment. A Data Impact Assessment takes a proactive approach, quickly identifying any data issues that may arise before the project/initiative launch. Topics such as noncompliance with government regulations or data loss when migrating data from one system to another are captured in the early stages. A DIA benefits organizations beyond compliance, sometimes mitigating monetary loss from project inefficiencies or money spent on regulatory fines and improper use of data.

2. Captures Robust Data Governance Requirements

Data governance requirements are often vast in scope. Thus, a DIA provides a one-stop shop for capturing the required data governance activities. Conditions such as Enterprise Data Lifecycle Management, Data Quality, Metadata Management, Data Lineage, Data Privacy, and many other requirements are all captured throughout the projects/initiative's lifecycle. A DIA also enhances a healthy data culture within your organization, emphasizing the importance of seeing data as an asset. Identifying and planning data management activities will ensure your project stays within timelines and budgets.

3. Reputational Impact

The reputational fallout of organizations that fail to capture, manage, and control their data accurately has been catastrophic and, in some cases, leaves a long-lasting impact on the trust and integrity consumers/clients, and other stakeholders have of these organizations. The increased use of data in this new age has also brought a heightened sensitivity around how organizations safeguard and manage the vast amounts of data in their possession. In many ways, a DIA captures loopholes that may attract risks of data breaches, improper data handling, and a host of data risks that may arise from the project/initiative.

4. Auditability

A data impact assessment documents, processes vital artifacts, and captures data governance requirements all in one place. Thus, this allows for ease of auditability internally or externally, creating accountability and transparency.

Components of A Data Impact Assessment

1. Project initiative/overview

The first phase of assessing a project/initiative through the lens of a DIA is to understand what the project entails from a data perspective. Understanding the core objective, its data source, data movement, and lineage, along with what stakeholders are involved. In this phase, measuring the quantity of data, the intensity of data migration, if any, and the risk that arises as a result are critical in the overview stage. Here are a few relevant questions worth asking in this phase below as follows:

- **Overview** - What does the project aim to achieve, and what are the core objectives?
- **Data Scope** - What data is relevant to this project? Where is the data sourced from? Are there multiple repositories/source data?
- **Project Contributors** - Who are the relevant stakeholders involved in this project (technology contributors, data owners, project managers, etc.)? What teams internally contribute to this project? What team is leading the project? Are there external third-party vendors involved? If so, what is the scope and involvement regarding the organization's data? Has said third party been assessed/vetted by the various Risk departments before proceeding?
- **Project/Initiative Data Usage** - What role does data play? Is there data migration taking place? What is the level/volume of data intensity involved? Is Data Migration taking place?

2. Data Risk Assessment

A DIA's Data Risk Assessment portion goes beyond the overview, provoking in-depth conversations about the project's data intensity. The Data Risk assessment encompasses a broad range of data governance requirements, including:

- **Regulatory Considerations:** Seeking to understand whether the project/initiative was created due to regulatory findings or purposefully designed to meet regulatory requirements will aid the project team in assessing if all those requirements are embedded within the project. Asking whether data created from this project will be shared with a regulatory body and if checks/validations are in place to ensure these requirements are met is critical.

- **Third Party Involvement:** Will this project create new/change existing third-party data exchange relationships? This is the pivotal question here, and if so, what does that entail and to what degree? What is a contractual agreement on data handling? Does the vendor have the capabilities to ensure alignment with the organization's data governance standards? Are all questions posed in the risk assessment.

- **Data Quality:** Identifying new data creation, uses of existing data, and its lineage helps assess data quality. Asking questions around whether existing data issues exist, and if so, how will they be addressed/managed, along with new data quality issues that arise. These questions ensure adequate data quality assessments take place before the project launch.

- **Enterprise Data Lifecycle Management**: Data Lifecycle Management deals with managing data from its inception to its usage and disposition. Questions around data classification, retention periods, and disposition capabilities will ensure that information assets are kept safe and secure.

- **Metadata Management:** Think of metadata as a tool that provides data about other data - a summary of a more extensive data set which gives it meaning and context. Ensuring metadata is captured for critical data elements enables efficient data utilization.

- **Data Privacy and Access Controls**: Identifying Personal Information within the project/initiative is critical to ensuring compliance with privacy requirements. Outlining access controls and setting authentication protocols will help bolster information assets' confidentiality and protection.

- **Artefact Collection**: Gathering key artifacts, documents, and process maps is essential to ensuring that all traceability of data handling and accountability of changes within the project scope are accounted for. Artifact collection also aids reference for future duplication or suitability when problem-solving.

3. Remediation Planning

Upon completion of the Data Risk Assessment portion, gaps, issues, and data risk areas are identified; thus, an action plan to remediate those gaps should be set in place. An action plan should include the following:

- **Gap Identification**: Identifying the root cause of the data risk, along with its source.
- **Risk Prioritization:** Rank gaps/issues by degree of impact on the data assets.
- **Action Plan:** Outline a timeline and step-by-step process to remediate the data risk gap. Factor in the project launch date, funding, feasibility, and stakeholders/owners required to execute the plan. Ensure adequate resources are in place to remediate the gap. Communicate this plan to all the necessary stakeholders.
- **Continuous Monitoring and Testing**: Tracking progress is essential, proactively monitoring and testing the remediation plan to ensure that due dates are met and that stakeholder tasks are actioned appropriately. Continually assess data risks that may arise due to changes in project scope, funding, or resource allocation.
- **Reporting:** Periodically report and inform all project/initiative stakeholders on the status of the remediation plan.

Conclusion

Ultimately, properly using a Data Impact Assessment often depends on the maturity of data governance within the organization, the data-driven culture, and awareness of the DIA benefits. A DIA should be treated as a living document, and continuous updates should be made at project/initiative tranches to ensure data risk is always captured. A Data Impact Assessment sets organizations on a proactive front of a data-driven culture. It will ultimately enable organizations to harness the power of data and change the perspective from a mere compliance tool to a necessary value-creation platform for data as an asset.