Why Data Governance needs to stop being overlooked

While Customer Experience (CX) analysis/design and Data Science have been embraced by business over the last decade, it surprises me how few organisations have managed to bring these capabilities together to really understand how to drive customer loyalty.

Data Governance has never been the most exciting of IT roles. As data scientists and analysts get all the attention for their complex algorithms and forecasts, data governance is often neglected or an after-thought. However there has been an increasing focus on this in recent years as governments around the world have been drafting new laws and regulations around how data must be stored, used, and shared. This is of particular importance for personally identifiable information (PII), financial information and healthcare information but applies to many other types of data that can be stored and used by organisations.

As data management experts, Fujistu Data & AI has always had a strong focus on data governance in the solutions that we design and deliver. Here we set out the framework that we use for ensuring that data in the data platforms that we deliver is effectively managed and governed.

To start with, we first need to be clear about what the term Data Governance means. Often organisations and individuals will have their own view of data governance which may cover any, or all, of the following capabilities:

- **Data Cataloguing** – Creating a register of all data items held by the organisation including detailed descriptions, ownership, creation information, storage information, usage information. This may also encompass recording data linage, data profiling and documentation of business rules.
- **Data Classification** – Documenting the sensitivity levels of data items held by the organisation.
- Data Security – Ensuring that data is only accessed by those that have a legitimate need and permission to do so.
- **Data Quality** – Ensuring that data held is of a suitable quality for the intended use and that issues and errors are rapidly identified and corrected.
- **Data Handling and Usage** – Defining rules for how data in the organisation is accessed and used.

- **Backup and Disaster Recovery** – Defining policies and approaches to ensure data is secured and can be recovered in the event of a system failure or major disaster.
- **Data Sharing** – Defining policies for how data can be shared with external organisations. This defines what data may and may not be shared. It may cover rules and processes for data de-identification and data masking that can enable normally sensitive data to be shared.

At Fujitsu Data & AI, we follow a seven-step approach to implementation of data governance solutions. Our approach is flexible, and we tailor the steps to the needs of each organisation based on the policies and processes are currently in place and the needs of the organisation.

Step 1 - Vision

This step defines what data governance means to the organisation. For example, a healthcare provider will typically require much stricter governance over data usage and access than would a manufacturing business. This should set out the key principles that underpin the usage of data within the organisation and goals for how it is to be governed.

Once the vision has been defined, it is important to gain executive agreement and sponsorship of it to ensure that the vision can be rolled out across the organisation.

Step 2 - Policies and Standards

Policies provide the rules that will ensure that the key principles of the vision are achieved. These define how data should be created, stored, accessed, and shared.

Standards should be defined that include naming standards and documentation standards. It is also often useful to define classification standards that can be used to describe how sensitive the data being held is – for example with data is Public, Internal, Sensitive or Restricted. The definition should also describe clear rules for how data is to be allocated to each of these classifications.

Once the policies and standards have been defined, they can be encapsulated into a Data Handling Guide that will provide documentation for those in the business on how data can be used and shared.

Step 3 – Operating Model

The operating model defines how the organisation will implement and manage the governance policies. Roles and responsibilities are defined for those with key knowledge or ownership of data. Some organisations may establish governance committees that meet regularly to review the rollout of governance at the organisation and look at revisions to policies and standards.

It is also generally useful at this step to establish a data asset register that records all the data assets held by the organisation along with owners of them, technical implementation, and users of the data.

Step 4 – Architecture

This step defines the technical approach to implementation of the governance policies. This defines how data is to be stored – for example in data lakes and data warehouses – how it may be accessed,

classified, and catalogued; how security will be implemented and how backups and recovery procedures are implemented.

The technical implementation of policies relating to data quality will also be defined in this step.

This step may also cover documenting how reference data and master data is stored, managed, and kept up to date.

Step 5 – Tool Selection

This step defines that tools that are to be used to implement the data governance policies and architecture. The broad nature often means that several tools may be required that cover data cataloguing, classification, lineage, modelling, sharing, quality. The organisational requirements from the tool should be documented then a selection process undertaken. Once the tools have been selected, they will need to be installed and configured to meet the organisations requirements.

Step 6 – Change Management

Once the policies, operating model and technical components are defined, they can be rolled out across the organisation. Those with roles as part of the operating model will need to be trained to ensure that they carry out their responsibilities correctly. Data handling standards should be rolled out to everyone in the organisation that uses data.

Step 7 – Compliance

The Compliance step ensures that the governance practices have been rolled out to the organisation are being correctly followed. This also reviews changes to the organisation and legislation to ensure that the policies, standards, and processes are kept up to date.

Following these steps will ensure that robust governance practices and processes are defined, rolled out effectively across the organisation and managed on an on-going basis.

To find out more, please contact a Fujitsu Data & AI specialist now.

Contact
Fujitsu Data & AI
+61 3 9924 3000