**Main Data Governance Roles- Owner, Steward, and Custodian**

In a data governance framework, **three key roles** are responsible for ensuring data is properly managed, secure, and used effectively:

**1. Data Owner**

**Who They Are:**

* A **senior-level business representative** responsible for the overall **accountability** of specific datasets.
* Typically someone from a **business unit** (e.g., Finance, HR, Marketing).

**Responsibilities:**  
✔ Defines **data policies and rules** (e.g., access permissions, retention).  
✔ Ensures data **aligns with business objectives**.  
✔ Makes decisions about **who can access and modify** the data.  
✔ Works with compliance teams to **ensure regulatory adherence** (GDPR, HIPAA).

**Example:**  
A **Finance Director** is the **Data Owner** for financial transaction records.

**2. Data Steward**

**Who They Are:**

* A **hands-on role** responsible for **data quality, accuracy, and governance compliance**.
* Often works in **IT, analytics, or business operations**.

**Responsibilities:**  
✔ Maintains **data accuracy, consistency, and completeness**.  
✔ Works with data users to **resolve issues** and ensure data quality.  
✔ Implements **governance policies** defined by Data Owners.  
✔ Monitors **metadata management** and **lineage tracking**.

**Example:**  
A **Business Analyst** in HR acts as a **Data Steward** by ensuring employee records are accurate and complete in HR systems.

**3. Data Custodian**

**Who They Are:**

* A **technical role** responsible for **data storage, security, and infrastructure**.
* Typically part of the **IT or Data Engineering team**.

**Responsibilities:**  
✔ Manages **data security, backups, and infrastructure**.  
✔ Ensures **data encryption and access control**.  
✔ Implements **data retention and disposal policies**.  
✔ Supports **data integration and ETL processes**.

**Example:**  
A **Database Administrator (DBA)** in IT is a **Data Custodian** ensuring the company's databases are secure and accessible.

**Comparison Table**

| **Role** | **Focus Area** | **Key Responsibilities** | **Example Position** |
| --- | --- | --- | --- |
| **Data Owner** | Business & Compliance | Defines policies, controls access, ensures regulatory compliance | Finance Director, HR Head |
| **Data Steward** | Data Quality & Governance | Ensures data accuracy, resolves issues, applies governance rules | Business Analyst, Data Governance Lead |
| **Data Custodian** | IT & Security | Manages storage, security, backups, and access controls | Database Administrator, IT Security Engineer |

**How They Work Together**

The **Data Owner** defines governance rules.  
The **Data Steward** enforces data quality and resolves inconsistencies.  
The **Data Custodian** ensures secure data storage and compliance with IT policies.

**Data Governance Roles in Different Industries**

The responsibilities of **Data Owners, Stewards, and Custodians** can vary depending on the industry. Below are real-world examples from **Healthcare, Banking, and Retail** to illustrate how these roles function in specific sectors.

**1. Healthcare Industry**

**Example:** A hospital managing patient medical records under regulations like **HIPAA** (Health Insurance Portability and Accountability Act).

| **Role** | **Responsibilities in Healthcare** | **Example Position** |
| --- | --- | --- |
| **Data Owner** | Defines access policies for Electronic Health Records (EHR), ensures compliance with HIPAA. | **Chief Medical Officer (CMO)** |
| **Data Steward** | Ensures patient records are accurate, cleans duplicate records, and monitors data integrity. | **Health Information Manager** |
| **Data Custodian** | Manages data security, encrypts patient data, ensures secure storage and backups. | **Hospital IT Security Lead** |

**Scenario:**  
A **Data Steward** ensures that patient John Doe’s record is not duplicated in the hospital's **Electronic Medical Record (EMR)** system. The **Data Custodian** secures this data, while the **Data Owner** ensures compliance with HIPAA.

**2. Banking and Financial Services**

**Example:** A bank managing customer transactions while ensuring compliance with **GDPR** and **PCI-DSS** (Payment Card Industry Data Security Standard).

| **Role** | **Responsibilities in Banking** | **Example Position** |
| --- | --- | --- |
| **Data Owner** | Defines policies for customer transaction records, ensures compliance with financial regulations. | **Chief Risk Officer (CRO)** |
| **Data Steward** | Ensures transaction records are complete, monitors fraud detection data. | **Risk Analyst / Data Governance Officer** |
| **Data Custodian** | Manages databases storing transaction logs, ensures encryption and access control. | **Database Administrator (DBA)** |

**Scenario:**  
A customer disputes a transaction. The **Data Steward** ensures accurate transaction records exist, the **Data Custodian** retrieves secure logs, and the **Data Owner** ensures policies are followed for dispute resolution.

**3. Retail and E-commerce**

**Example:** An e-commerce company managing customer purchases, inventory, and marketing data while complying with **CCPA** (California Consumer Privacy Act).

| **Role** | **Responsibilities in Retail** | **Example Position** |
| --- | --- | --- |
| **Data Owner** | Defines policies for customer data usage in marketing campaigns, ensures compliance with CCPA. | **Head of Customer Insights** |
| **Data Steward** | Ensures customer addresses are correct, prevents duplicates in loyalty programs. | **CRM Manager / Business Analyst** |
| **Data Custodian** | Manages cloud databases storing customer purchase history, ensures real-time inventory updates. | **Cloud Engineer / IT Security Manager** |

**Scenario:**  
A customer requests their personal data to be deleted under **CCPA**. The **Data Steward** verifies the request, the **Data Custodian** removes the data securely, and the **Data Owner** ensures legal compliance.

**Key Takeaways**

✅ **Healthcare** → Ensuring patient privacy and compliance with HIPAA.  
✅ **Banking** → Managing transaction accuracy and financial security.  
✅ **Retail** → Protecting customer data and ensuring personalized experiences.