Catena-X

THE FIRST OPEN AND COLLABORATIVE DATA ECOSYSTEM

DATA GOVERNANCE GUIDE

Basic Governance Principles for Cross Company Data Exchange

Release V2, October 2023

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Catena-X

TABLE OF CONTENTS

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Abstract

From an ecosystem perspective, this document highlights governance mechanisms for providing and consuming data to or from third parties. We focus on processes and exemplary roles in an organization required to govern and manage a Data and Analytics Ecosystem that spans functions, departments and third parties. In the broader sense, the target audience this document wants to address includes data providers and data consumers participating in the ecosystem in general.

It should be mentioned that the Governance Guide was designed from the perspective of large companies. Small and medium sized companies can make concrete simplifications based on this good governance practice in accordance with their organizational structure.

In the narrow sense, the target audience includes specifically

1) Data & Analytics Roles

2) Governance Roles.

Thereby Data & Analytics Roles represent roles directly involved within the Data & Analytics Value Chain, either in a core or supporting role. Therefore, Data & Analytics Roles perform operational activities (e.g., developing and maintaining Assets, Use Cases and IT applications), directly contributing towards a sustainable data ecosystem. Supporting Data Governance Roles provide guidance for Data & Analytics Roles on how to perform activities of the Data Value Chain in a compliant manner. Hence, those roles translate internal and external norms and regulations into binding policies and standards which can be applied in practice.

Management Summary

Catena-X is pursuing the goal of creating the first data-driven value chain. The prerequisite for this is that all partners have aligned data governance processes focusing on data provisioning and data consumption. This document outlines the transferability of universal governance requirements to data exchange scenarios (like, for example, GDPR, information security, antitrust law, data strategy etc.) to ensure compliant data provisioning and consumption in the Catena-X data space.

The following nine Guiding Principles for Governing Data Exchange Processes have been identified. In order to act as a data provider or consumer and trusted participant in Catena-X, it is expected from all participants to have processes and people in place to ensure the adherence to those principles. Additionally, these guiding principles listed below not only contribute to Catena-X but also serve as a governance guideline for the partner companies themselves.

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

1. **Adhere to the 10 Golden Rules[1] for all participants in the network**

The Catena-X Data Space is a secure and standardized data ecosystem. Participants in this ecosystem must adhere to these basic ten principles.

2. **Follow guidelines for data privacy, information security, antitrust compliance and IT Security**

Adhering to guidelines for data privacy, information security, antitrust compliance, and IT security ensures safeguarding sensitive information, promoting fair competition, and protecting digital assets against unauthorized access and cyber threats.

3. **Establish Data Governance roles supporting the data release process**

Data Governance roles ensure proper oversight, accountability, and adherence to protocols when sharing data, maintaining data integrity, and mitigating potential risks associated with data dissemination.

4. **Define which company roles or entities are responsible for data (e. g. data semantics) and IT (e. g. data pipelines) approval decisions**

Clearly designating responsible company roles ensure accountable decision-making, streamlines enabling IT processes like developing and operating data pipelines and IT infrastructure, and maintain the alignment between stakeholders for efficient and secure data management.

5. **Ensure agreed data quality by regular quality checks**

Ensuring consistent data quality guarantees that data remains accurate, reliable, and actionable, fostering informed decision-making and maintaining the trustworthiness of the information used.

6. **Ensure compliance with data storage requirements such as retention period, SLAs, data location, data availability and accessibility**

This commitment assures that data is retained appropriately, service levels are met, and data remains available and accessible as needed, aligning with regulatory standards and organizational needs.

7. **Ensure logging and monitoring of released and consumed data**

Enforcing logging and monitoring provide a comprehensive record of data activities, facilitating traceability, identifying potential anomalies, providing customer support, and enhancing overall data security and accountability.

[1] Catena-X | 10 Golden Rules

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

8. **Enable efficient cross company data processing by balanced need-to-know and proud-to-share approach in Strategy and Management Systems**

Companies are looking towards reshaping their data management operating model and IT management model to focus on data sharing. And need rethinking. . Upfront marking of uncritical data can facilitate quicker data exchange, along with other measures such as defining approval patterns and transparent reporting. Reshaping the data strategy and architecture is also important in balancing data protection and sharing. A balanced approach to data management can bring great benefits to businesses such as higher efficiency and improved decision-making.

9. **Enable efficient data handling with ecosystem partners by companywide meta data management and semantic hubs.**

Businesses need to create integrated data catalogs comprising data definition, compliance, and usage information to facilitate efficient and agile data exchange scenarios with other companies. The meta data in the data catalogs should be managed through machine-readable semantic hubs to avoid creating use-case specific interfaces with independent data definitions and semantics.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Finanziert von der Europäischen Union
NextGenerationEU

1. INTRODUCTION

Organizations can capitalize on collaborating with partners in ecosystems, but there is also a risk of losing control on data, granting unsecured access to information, or providing low-quality information.

In the exemplary case that BoM data is shared with third parties there is a risk that partners have not established security and control measures to safeguard the data, leading to unauthorized use or distribution of information. This can compromise the confidentiality, integrity, and availability of the data, which can negatively impact the vehicle's life cycle. Sharing BoM data with third parties may also inadvertently expose the data to potential cyber threats. Third parties may not have adequate security measures in place to prevent data breaches, unauthorized access, or other malicious activities that can compromise the BoM data's security. Additionally, sharing incomplete or inaccurate BoM data with third parties can affect the quality and reliability of the product (e. g. vehicle). Low-quality data can lead to delays, errors, and safety issues that can negatively impact the product's performance, safety, and durability.

To deal with these issues and support the objectives of a shared ecosystem, inter-organizational data governance mechanisms need to be established. These mechanisms can be grouped into the three areas of data management processes, data governance policies and IT governance policies.

Data management processes encompass various aspects of handling data. This includes defining specific roles and their respective responsibilities. In addition, data policies provide rules for the creation, control, management, and audit of data. The development of data standards is particularly important for the inter-organizational exchange of data. These standards define, for example, how data is handled and how it is represented to ensure that the required quality criteria are met.

Data governance policies target the methods to regulate data inside and outside the organization. On the one hand, this involves establishing processes and procedures for data use and data flow. On the other hand, the setting for data provisioning and data sharing is defined. In this way, the sharing of data between two or more organizations is controlled, including the (semantic) descriptions of the data, the data flow, and the obligations for providers and users through legal and data governance terms.

IT governance policies are established to address the complexities of managing digital data contracts and ensuring appropriate data flows. This can be achieved by leveraging technology with its ability to automate and scale the implementation of standards, processes, and rules.

This guide does not cover all the essential steps (e. g. pre-clarified cooperation alignment and establishment of a basis of trust between data exchange partners) for end-to-end onboarding to Catena-X. Instead, it focuses on the relevant aspects related to data exchange. The respective process steps are described as a user journey (see Figure 1). Two different perspectives of the data provider and the data consumer are taken. This concerns the process from the design and formulation of the data request to consumption, logging and monitoring. It also identifies general

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

requirements that need to be met in order to prepare for data exchange and provides a number of templates that can be helpful in communicating and preparing for each step of the user journey.

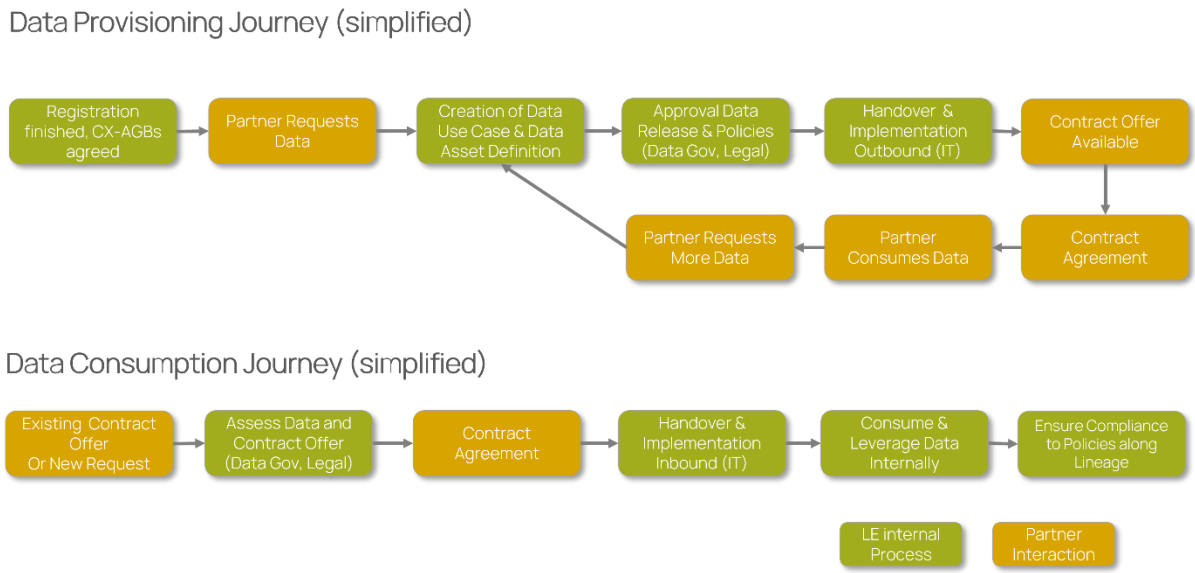

Figure 1. Data provider and Data Consumer simplified Journey

2. PREREQUISITES

This section describes the prerequisites that must be fulfilled by a partner (consumer and provider) before participating in a data exchange. The actual data exchange process begins after the basic requirements have been fulfilled.

2.1 Joining the Catena-X Data Space in the Role of Participant

The following items list some of the basic **prerequisites for both partners** and need to be completed to allow for data exchange within the Catena-X Data Space.

- Catena-X Governance Framework[2] acknowledged and adherence to, e. g. 10 Golden Rules, confirmed
- Registration with an Operating Company completed (incl. necessary Agreements signed)
- BPNs exist (received upon successful registration)
- EDCs configured
- Roles and contact persons defined and aligned (see also Appendix A. Assisting Roles & Responsibilities)
- Use Case Frame Conditions acknowledged and signed by signing authority

A basic overview of contracts or agreements that need to be agreed between different parties in Catena-X (Association, Operating Company, Data Exchange Partners) can be found in Figure 2. These range from bilateral contracts on the delivery of parts / components to agreements of each

[2] Catena-X | Governance Framework for Data Space Operations

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

partner with an Operating Company on the participation in Catena-X to Use Case specific Frame agreements. An actual data contract will in the end be negotiated electronically via the respective EDCs.

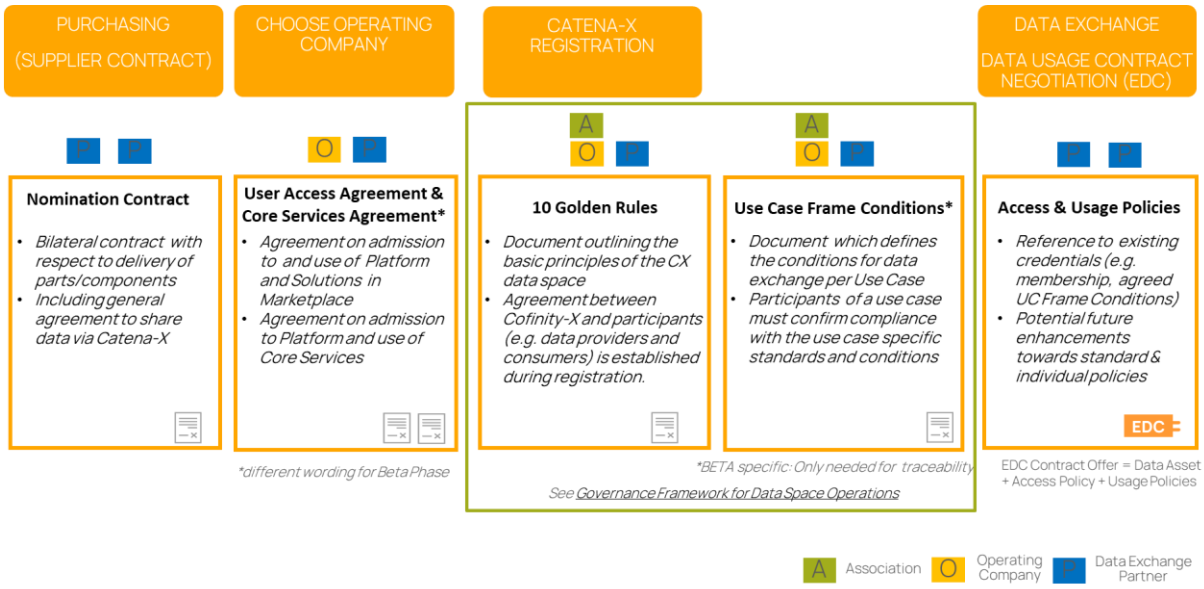

Figure 2. Overview of agreements (as of September 2023)

2.2 Logging Concept

In addition concepts for data logging /logging of data transactions is seen as a prerequisite in the context of data exchange (provider and consumer). It should at least be logged which partner company consumed which data asset. These logging protocols can help to create transparency regarding regulatory requirements and incident management support. For more information on logging types, we refer the reader to Appendix B. Types of Logs.

3. DATA PROVISIONING PROCESS GUIDELINE

3.1 Asset Creation and Approval

Assuming that a data request has been received from a partner, this process step illustrated in Figure 3 describes the requirements for creating a data use case and the required data assets from the data provider's perspective. In addition, the plausibility of whether and how the corresponding data request can be initially approved and implemented is checked.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Finanziert von der Europäischen Union
NextGenerationEU

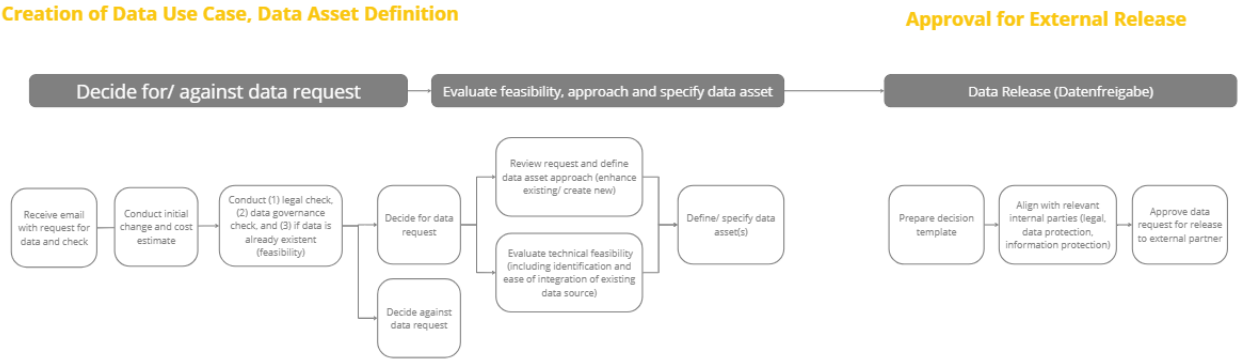

Figure 3. Asset Creation and Approval process

3.1.1 Creation of Use Case and Data Asset Definition

- Data request by data provider and internally distributed to corresponding data management function (e. g. data steward, see Appendix A. Assisting Roles & Responsibilities)
- Initial check conducted to decide whether the data request should generally be rejected (e.g., personalized data, low quality data or economic feasibility) or is generally safe and can go through the data approval process
- Full legal and data protection check conducted (approved by legal team if required)
- Additional data governance check conducted (e. g. compliance with antitrust law, alignment with companies' data strategy)
- Data availability and feasibility check conducted
- Cost analysis conducted to estimate costs associated with data request (e.g., data preparation, pipeline development and operations, storage and compute costs)
- High-level data transfer solution design developed by use case owner and IT
- Source system identified and attributes mapped

3.1.2 Approval for External Release

- Approval Decision template filled out and relevant stakeholders for decision identified
- Data request approved by decision board (if required - depended on organizational roles and responsibilities, see also Appendix C.1. Board Decision – Definition (a) use case and data information template (b) and decision documentation template (c))

3.2 Preparation and Deployment

Assuming an approval is granted, this process step describes the internal data pipeline requirements definition, the operational implementation and test management for the technical implementation of the data exchange according to Catena-X standards.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Finanziert von der Europäischen Union
NextGenerationEU

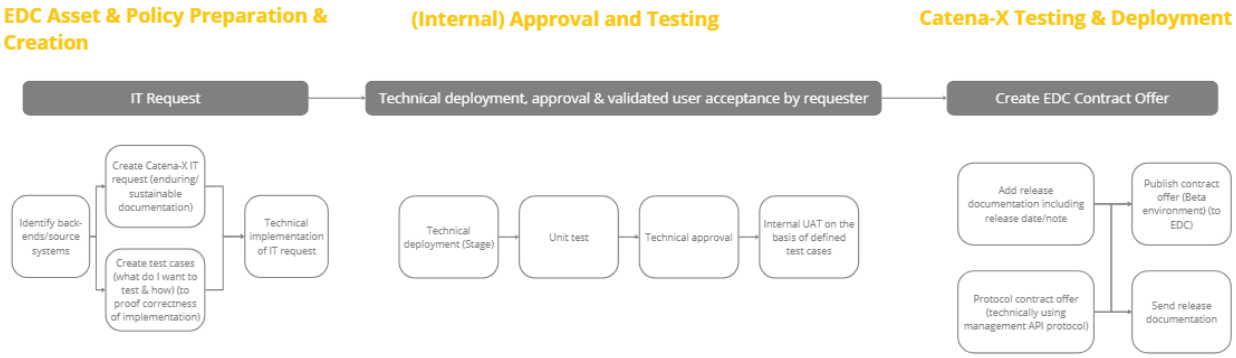

Figure 4. IT preparation and deployment process steps

3.2.1 EDC Asset & Policy Preparation & Creation

- IT request template filled and submitted to IT department (see also Appendix C.2. IT Request Template)
- Test cases created test scenarios/user acceptance criteria defined (see also Appendix C.3. Test Cases Checklist)
- Detailed solution design developed by IT team
- Data prepared and aggregated from source system and mapped to Catena-X standard data model
- End-to-end data chains internally tested and handed over to product owner
- IT compliance and security checks conducted for IT System (see Appendix D. IT Governance / Compliance Appendix C. Supporting Templates for details)
- Operational readiness ensured

3.2.2 (Internal) Approval and Testing

- IT request technically deployed
- Use case specific and prior defined tests conducted
- Usage and access policies for data asset checked
- Data quality (also check against quality requirements specified by partner) and user acceptance checked

3.2.3 Catena-X Testing & Deployment

- Requested data checked and approved by data exchange partner
- Release documentation including release date/note added and sent to data exchange partner
- Contract offer protocolled (management API protocol) and published
- Logging Concept in place (Server Logs, Customer Support Logs, Audit Logs, Offer and Agreement archive – See Appendix B. Types of Logs)
- Data Integration Patterns Guide[3] checked, and logging/monitoring requirements aligned

[3] Catena-X I Data Integration Patterns Guide

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

4. DATA CONSUMPTION PROCESS GUIDELINE

The prerequisites for data exchange are the same for providers and consumers (see Section 2). The process begins here with the description of the data requirements by the data consuming partner (see Figure 5).

4.1 Define Data Need

- Data request internally defined and aligned (e. g. with use case owner and supporting roles, see Appendix A. Assisting Roles & Responsibilities) (see also Appendix C.4. Data request exemplary for the UC Traceability.)
- Data request information send to data provider (existing contact, e.g., key account manager)

4.2 Data Consumption

This process step illustrated in Figure 6 aims at the consumption and further use of data under consideration of the rules (policies) agreed with the data provider (partner).

A Company needs to ensure technically and organizationally that policies are complied with internally (by consumers) and processes for compliance violations must be in place to ensure violations can be reported and followed-up on. This may also include deletion concepts of data based on framework agreements or policies.

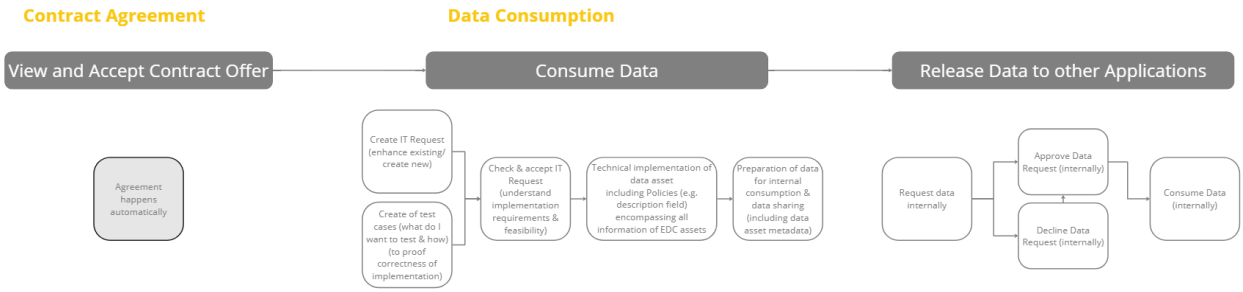

Figure 6. Contract agreement and data consumption process

4.2.1 Contract Agreement - data offer review and acceptance

In this step the partners close a legally binding contract. Only if both sides have defined and agreed policies that match each other, an EDC can negotiate contracts automatically. Thus, as a Data Consumer I must ensure to orchestrate the EDC(s) and implement a Business Service to check for any individual rules or purpose defined by the Data Provider in their offer. In this case, it must be ensured to manually check these rules and only in case of acceptance trigger negotiation.

4.2.2 Data Reception

- Internal IT request and test cases created (see also Appendix C.2. IT Request Template)
- IT request checked and accepted

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

- Data asset technically implemented
- Data prepared for internal consumption & data sharing
- Compliance with internal governance criteria ensured
- Validation to ensure that the provided data matches the specifications outlined in the data request
- Acceptance or trigger modification of the data exchange

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

5. APPENDIX

The appendix serves as a supplementary section that provides additional information related to the main content of the governance guide including:

Appendix A. Assisting Roles & Responsibilities: Data governance involves the establishment of roles and responsibilities within an organization to ensure the effective management, quality, security, and compliance of data throughout its lifecycle. This template provides guidance on possible supporting governance roles that can be filled in companies.

Appendix B. Types of Logs: There are several reasons for data logging: Anti-trust law, Use Case Relevance, Information Protection. Audit logs are used for reporting and monitoring purposes to provide governance bodies with information (e. g. policies, asset values, tracking of data exchange progress). The template provides exemplary categories for logging and monitoring.

Appendix C. Supporting Templates: At various stages during the data exchange journey, there are steps that require definition of requests with respect to data and metadata, logging, test cases or decisions. The templates provide some guidance for structuring these as part of communication between partners or between business and IT, or as a basis for implementation.

Appendix D. IT Governance: IT Governance is crucial for managing and ensuring the effective and secure operation of an organization's IT applications. They involve establishing frameworks, policies, processes, and procedures to ensure that the organization's IT operations align with its business objectives, legal requirements, and industry standards.

Appendix A. Assisting Roles & Responsibilities

It is difficult to standardize governance roles as each company has its own goals, values and culture that need to be considered during the data exchange process. Governance also encompasses a variety of areas such as compliance, risk management, financial management and IT security, which may vary in different organizations. In addition, the size and complexity of an organization can affect the implementation of governance roles. A small and medium sized companies (SMEs) may have less complex governance structures than a large multinational company. It may therefore be that the roles' fields of activity overlap or are merged to reduce complexity. Therefore, it is important that each organization tailors its governance roles and responsibilities to its specific needs and objectives.

However, we would like to provide a basis for possible process support roles and their tasks in Table 1, which can be adapted or adjusted depending on the company setting:

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Table 1. Assisting Roles & Responsibilites

Role	Function	Exemplary Tasks and Responsibilities
Use Case Owner (internal)	The Use Case Owner is internally responsible for one or more data use cases within the company and is responsible for their success.	- Defines and requests the required data - Coordinates with relevant internal stakeholders, such as the Data Steward and Data Engineer - Conducts business cost-benefit assessment and analysis - Defines and validates IT requests (consults Data Pipeline Lead) through User Acceptance Testing (UAT)
Data Pipeline Lead	The Data Pipeline Lead is responsible for gathering IT requirements for Catena-X/EDC data assets and policies.	- Assesses requirements and assists Use Case Owner in finding appropriate source systems - Steers the implementation of inbound and outbound data pipelines - Responsible for IT compliance and security topics
Data Engineer	The Data Engineer is responsible for gathering and implementing technical requirements (e.g. by developing data pipelines towards Catena-X/EDC).	- Creates/Implements data assets and policies technically - Conducts functional mapping of data assets (data models) - Builds interfaces to EDC

Role	Function	Exemplary Tasks and Responsibilities
		- Ensures data quality via unit and integration tests
Data Steward / Data Owner	The Data Steward ensures data management, quality, and security, aligned with the business team (e.g. responsible for data releases towards Catena-X). They typically have a business background and IT skills.	- Manages data from a variety of sources - Responsible for quality of the data gathered - Documents and enforces governance rules around data collection, storage and use - Executes Corporate Data Governance policies and standards - Develops and enacts processes and procedures for data management and security
Data Management Governance Function (DMGF)	The DMGF is responsible for decentralized data management and governance functions.	- Advises on data management and usage guidelines across business domains - Approves use cases - Consults the Use Case Owner in data usage - Sets up and controls processes to manage all life cycle phases of the data - Establishes processes for supporting Data Consumers and Data Product Owners

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Role	Function	Exemplary Tasks and Responsibilities
Data Product Owner	A Data Product Owner is accountable for Data Product(s) and is the product manager for this Data Product(s).	- Identify data which is necessary to fulfill the business needs - Initiate demand for Product / Use Case creation - Define Service Level and Data Quality for the Data Product according to the requirements - Determine data classification and Information Protection in accordance company internal policies - Manage Data Product Lifecycle - Define general usage rules for the Data Product
Supporting Roles	Supporting roles will be needed in various process steps.	For example: Purchasing / Sales, Legal, Signing Authority, Decision Board, RollOut Manager

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Appendix B. Types of Logs

Extended Server Logs

- Technical logs
- For Debugging, Monitoring, Security
- Retention: 7-14 days

Audit / DTO Metadata Logs

- The who/what/when/where
- Track consumption and understand changes
- Retention: Up to six months

Logs for Customer Support

- Understandable by non-experts
- Tells the customer what to do next
- Retention: 30 days or until issue resolved

Archive of Offers and Agreements

- For antitrust and compliance
- Proof who had access to assets
- Retention: 10 years

Appendix C. Supporting Templates

Appendix C.1. Board Decision – Definition (a) use case and data information template (b) and decision documentation template (c)

Template for initial data release approval of new data assets and for subsequent changes that require exceptional approval.

Release information

- Information level: Use Case
- Frequency: once per PI / quarter (if required, see below)

Recommendation

- Short-term: Main Departmental Steering Committee
- Medium-term: Data release via dedicated governance board

Scenario	Description	Example / Scope	Approval by

Initial release	Definition of the scope of the release (subsequent extensions within this framework do not require renewed board approval)	• Catena-X data aspects / semantic models
		• Whitelist / Blacklist of partners (Access Policies)
		• Data Assets and (minimal) Usage Policies
		  • Provision for period X
		  • Columns (& rows) like Geolocation, Derivatives
			Board

Changes / Extensions	New feature / new attribute	e.g. other properties • Update Information Security and Data Protection requirements • Data preparation Pipeline Data Lake → EDC Asset	Board
	New position	e.g. new components • Linkage to e.g., existing digital twins • Data preparation Pipeline Data Lake → EDC Asset	Department UC Owner (internal) & Data Steward
	Deviation from the agreed "scope"	e.g., further geolocations, new derivatives	Board

(a)

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case

#Insert information

Data Asset (e.g., Data Lake)
#Insert information

Description
#Insert information

Access Policy
#Insert information

Usage Policy
#Insert information

Data Asset Preparation
- ❑ Done/no need for preparation
- ❑ Needs to be prepared

(b)

Data Request Background Information

#Insert general information on data request

Data Request Specification (e.g., initial release/new feature/new attribute or deviation from agreed scope)
#Insert information

Purpose of Data Request
#Insert information

Description of Data Usage
#Insert information

Start, Duration, End of Data Storage
#Insert information

Frequency
#Insert information

Requestor Target Group
#Insert information

Board Decision

Date and Time
#DD.MM.YYYY at HH:MM

Board Members
#Please list all board members here

Board Decision

The board decided to…

- ❑ Fulfill the data request
- ❑ To not fulfill the data request

(c)

Board Decision Template.pptx

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Appendix C.2. IT Request Template

Template to query the data provision process from IT, which bundles all necessary IT request information.

Use Case Name
#Insert information

Date
#DD.MM.YYYY

Requesting company
#Insert information

Requestor (e.g., Person, Department, Business Function)
#Insert information

Request Recipient
#Insert information

IT Request Information (if already known)
#Insert information (specification e.g., Catena-X data request template)

#Name / #Date and Time

_____

Details	
Project ID	#Insert information
Project Title	#Insert information
Asset*/Data	#Insert information
Access Policies**	#Insert information
Usage Policies**	#Insert information
Whitelist Member	#Insert information
Blacklist Member	#Insert information
Non-Functional Requirements (e.g., Frequency, Security)	#Insert information
Cost Center	#Insert information
Data (Product) Owner/ Data Steward	#Insert information
Domain Expert(s)	#Insert information
Due Date	#Insert information

*If existing, otherwise please specify what new asset is needed
**Catena-X related

IT Request Template.pptx

Appendix C.3. Test Cases Checklist

Template/checklist for the definition and conduction of test cases/test scenarios.

- ❑ **Step 1:** Double check if all prerequisites to connect to the Catena-X data space are fulfilled (link onboarding guide, technical guide, Catena-X connectivity tests)
- ❑ **Step 2:** Execute unit tests for every unit of the data provisioning pipeline i.e., from data source to data sink where data is made available for Catena-X use cases
  - ❑ Validate if every unit provides the expected results
  - ❑ Acceptance of each unit test by responsible role (e.g., test manager, data steward, data owner, data product owner)
- ❑ **Step 3**: Execute end to end test of the data provisioning pipeline on test systems (if available)
  - ❑ Validate if the whole pipeline running and provides the expected results
  - ❑ Acceptance of e2e test responsible role (e.g., test manager, data steward, data owner, data product owner)
- ❑ **Step 4:** Rollout of the data provisioning pipeline to productive systems and run the pipeline end to end
  - ❑ Check if the data is available in the defined data sink
- ❑ **Step 5:** Final check and approval by responsible role to publish data asset(s) to Catena-X
- ❑ **Step 6:** Publish assets in Catena-X (register them in the digital twin registry
  - ❑ Quick check if data asset is registered correctly

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Test Cases Checklist Template.pptx

Appendix C.4. Data request exemplary for the UC Traceability.

Template that provides guidance on how to specify data requests towards your partner in the context of Catena-X. Usually this is initially communicated by Key Account Management or Purchasing Departments and contains among others information on relevant components, purpose, usage, frequency and related standards and required data formats (semantic models).

- Purpose of the Data Request
  - Aufbau von Datenketten für Fahrzeuge und Getriebe, um die in Catena-X entwickelten Komponenten mit Realdaten zu verproben (BetaPhase bis Ende 09/2023). Die Datenkette dient zukünftig der schnelleren und zielgenaueren Eingrenzung bei Qualitätsthemen und ist Grundlage für einen weiteren Komponenten-bezogenen Austausch.
- Description of Data Usage
  - Gemäß der Catena-X Use Case Rahmenbedingungen* (Nutzung im Rahmen des Catena-X Use Cases Traceability für Qualitäts-Analysen, Technische Aktionen
- Start, Duration and End of Data Storage
  - Gemäß der Catena-X Use Case Rahmenbedingungen* (bis Ende Beta-Phase, Ende 09/2023)
- Frequency of Data Provisioning
  - Anlage & Veröffentlichung Digitaler Zwillinge in Digital Twin Registry zeitnah nach Produktion der physischen Komponente -> spätestens am Ende des Tages (-> Tagesproduktion, Nachtlauf)
- Processing of Notifications ("Anfragen")
  - Reaktionszeit auf Anfragen gemäß des in der Nachricht hinterlegten Datums
  - Für Betaphase: innerhalb von x Arbeitstagen
- Existing Data Exchange Agreements
  - Partner tauschen in vielen Projekten gegenseitig Daten aus (u.a. Entwicklung, Einkauf, Qualität)
  - Geeignete bestehende Regelungen: **** (e.g. Leistungsvereinbarungen, Standards, ….)
- Requestor Target Group
  - Betaphase: BMW Use Case- & Projektmitarbeiter (insbesondere Abteilungen ***, ***)
- Requestor Contact Person
  - <Name, Abteilung>
- Rel. Data Formats / Semantic Models / Standards
  - Currently valid Catena-X Standards (refer to https://catena-x.net/de/standard-library)
  - CX-**** Aspect Model: ****
  - CX-**** Aspect Model: ****
  - Also see subsequent slide (Data Mapping)

Data Request Template.pptx

Appendix D. IT Governance / Compliance

IT Policies and Compliance:

Developing and communicating IT policies and standards is essential for guiding IT operations and ensuring compliance. Regularly reviewing and updating policies is crucial to address evolving regulatory (e. g. GDPR) and security requirements. Regular reviews ensure that policies remain relevant, aligned with industry best practices, and compliant with applicable laws and regulations. This helps mitigate risks and demonstrates a commitment to maintaining a strong and secure IT environment.

Conducting audits and assessments is an integral part of ensuring adherence to IT policies and compliance with regulations. Audits help evaluate the effectiveness of controls, processes, and procedures, and identify any gaps or areas of non-compliance. They involve examining IT systems, infrastructure, and practices to ensure that they meet the requirements specified in the policies

and regulatory frameworks. Assessments may also involve external audits/Catena-X audits or certifications to validate compliance with industry standards or legal obligations.

IT Service Management:

IT service management (ITSM) involves defining and implementing processes and practices to deliver and support IT services effectively. These processes include incident management, problem management, change management, and service request management.

Monitoring and improving service delivery processes is crucial to maintain high-quality service levels. This includes measuring and analyzing metrics such as response times, resolution times, and customer satisfaction. Regular monitoring allows organizations to identify areas for improvement, optimize resource allocation, and make informed decisions to enhance service quality.

Establishing service level agreements (SLAs) and metrics helps set expectations and measure service performance. SLAs define the agreed-upon levels of service to be provided by IT to the business or end users. Metrics associated with SLAs, such as response times or uptime percentages, enable organizations to track and report on their performance against agreed-upon targets.

Information Classification for IT Application:

Information classification is crucial for IT Application because it helps identify and categorize the sensitivity and criticality of the information handled by the application. By classifying information, organizations can determine the appropriate security controls, access restrictions, and data handling procedures required to protect sensitive data. It enables organizations to allocate resources and prioritize security measures based on the importance and risk associated with different types of information.

IT Security Documentation:

IT Security Documentation refers to the collection of documents that outline the security measures, controls, and procedures implemented within an IT application. These documents provide a comprehensive view of the security architecture, infrastructure, and policies governing the application. They serve as a reference for understanding the security requirements, identifying potential vulnerabilities, and ensuring compliance with industry standards and regulations. IT Security Documentation plays a vital role in documenting the security posture of the application and guiding security-related decision-making.

IT Security Conformity Statement:

The IT Security Conformity Statement is a formal declaration or report that assesses the compliance and incident management of an IT application with predefined security requirements, standards, and regulations. It involves evaluating the application's security controls, identifying any gaps or vulnerabilities, and reporting associated risks. The statement provides transparency regarding the

Finanziert von der Europäischen Union
NextGenerationEU

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

security status of the application and highlights any areas that require attention or remediation. It helps demonstrate adherence to security standards and assists in regulatory compliance efforts.

Penetration Test:

A Penetration Test, often referred to as a "pen test," is a controlled simulated attack on an IT application to identify vulnerabilities and weaknesses in its security defenses. This proactive security assessment aims to identify potential entry points for attackers, discover vulnerabilities, and evaluate the application's resistance to various attack techniques. By conducting penetration tests, organizations can gain insights into the effectiveness of their security controls, prioritize remediation efforts, and ensure the application is resilient against real-world threats.

IT Application Clearing:

IT Application Clearing typically refers to the process of obtaining necessary approvals or clearances for an IT application, often in the context of regulatory compliance or legal requirements. Depending on the specific industry or jurisdiction, certain applications may need to undergo clearance procedures to ensure compliance with relevant laws, regulations, or policies. This process involves evaluating the application's compliance with specific criteria, such as data privacy, security standards, or industry-specific requirements. IT Application Clearing ensures that applications meet the necessary compliance obligations and minimize any legal or regulatory risks.