Software Requirements Specification

for

Gaia-X Federation Services Compliance Documentation Service IP.CDS

Published by

eco – Association of the Internet Industry (eco – Verband der Internetwirtschaft e.V.)
Lichtstrasse 43h
50825 Cologne
Germany

Copyright

Table of Contents

List of Figures

List of Tables

1. Introduction

To get general information regarding Gaia-X and the Gaia-X Federation Services please refer to [1] and [4].

1.1 Document Purpose

This document covers the Compliance Documentation Service. To show that a Federation Service fulfils all defined requirements, the provision of appropriate evidence is necessary. This evidence can be delivered in different types (e.g. specifications or concepts, test reports or certificates). The Compliance Documentation Services specifies how the fulfillment of Security and Privacy by Design has to be documented by each Federation Service.

1.2 Definitions, Acronyms and Abbreviations

Federation Services
Federation Services are grouped into the four domains “Identity and Trust” (WP1), “Federated Catalogue” (WP2), “Sovereign Data Exchange” (WP3) and “Compliance” (WP4)[1].

Abbreviation	Term
AISBL	Association internationale sans but lucratif
API	Application Programming Interface
CSIRT	Computer Security Incident Response Team
EUCS	European Cybersecurity Certification Scheme for Cloud Services
FIRST	Forum of Incident Response and Security Teams
GDPR	General Data Protection Regulation
IDR	Incident Detection and Response
PII	Personal Identifiable Information
SDLC	Software Development Lifecycle
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operation Center
SoC	Statement of Compliance
SoPC	Statement of Partly Compliance
SoNC	Statement of Non-Compliance
SoNA	Statement of Not Applicable
SPBD	Security and Privacy by Design
TI / TIP	Threat Intelligence / Threat Intelligence Platform
UI	User Interface

[1] Please refer to appendix B for an overview and explanation of the Work Packages (WP)

Table 1 Definitions, Acronyms and Abbreviations

1.3 References

[1] Gaia -X: Technical Architecture, Release 21.03;
Please refer to annex “Gaia-X_Architecture_Document_2103”
[2] ENISA EUCS Scheme; https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme
[3] Gaia-X - Specification of non-functional Requirements – Security and Privacy by Design
Please refer to annex “GXFS_Nonfunctional_Requirements_SPBD”
[4] Gaia-X, European Association for Data and Cloud, AISBL (2021): Gaia-X Policy Rules Document
Please refer to annex “Gaia-X_Policy Rules_Document_2104”
[5] Gaia-X Federation Services Technical Development Requirements
Please refer to annex “GXFS_Technical_Development_Requirements”

1.4 Document Overview

The second chapter describes the Compliance Documentation Service including the functional service description, interfaces and, if already defined, service requirements.

1.5 Interaction with other Federation Services

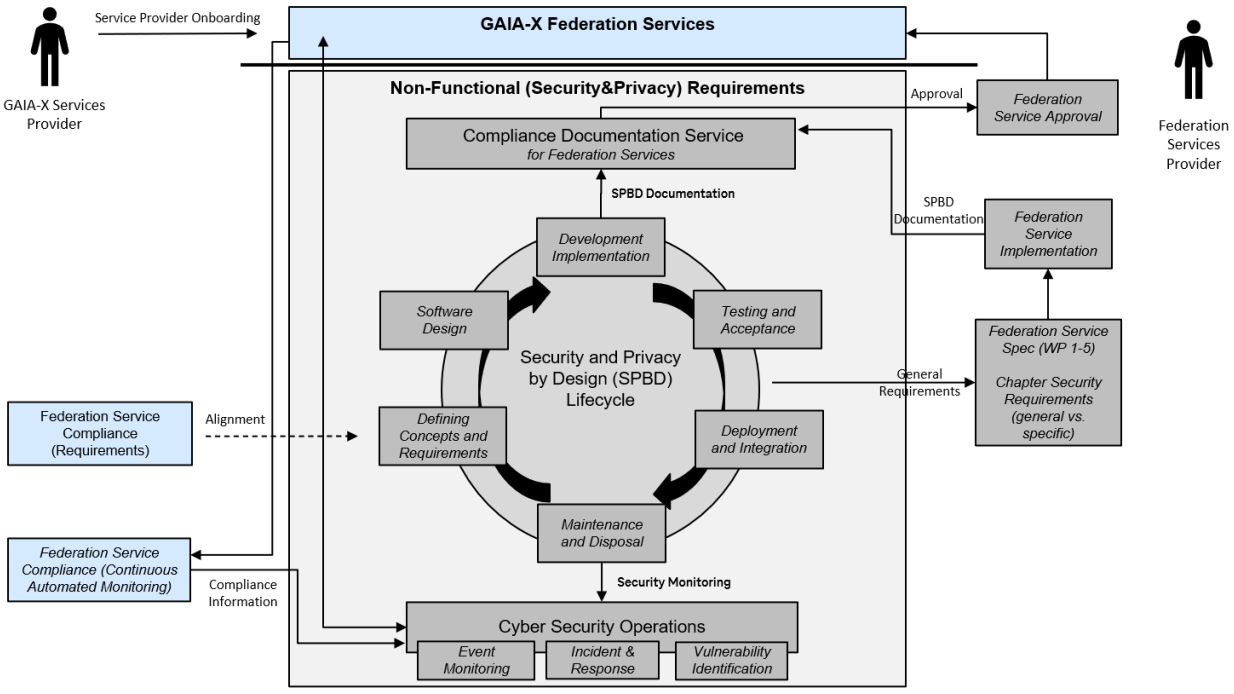

Figure 1: Interaction of Security and Privacy by Design with other services

The Security and Privacy by Design process for Gaia-X Federation Services defines requirements and deliverables that have impact on the Compliance Documentation. The Federation Service provider must deliver security and privacy documentation which will be stored in the Compliance Documentation Service.

2. Product Overview

The Compliance Documentation Service aims to support the Security and Privacy by Design process which is described in [3]. Federation Service Providers shall use the service to state and prove compliance of the enabling Gaia-X Federation Services, e.g., the Federated Catalogue, the Gaia-X Portal, etc., to the Gaia-X requirements (cybersecurity, data privacy). On the other hand, a Gaia-X Authority (or an accredited entity on behalf of Gaia-X) can verify and assess the provided compliance information and approve the Federation Service implementation to go live.

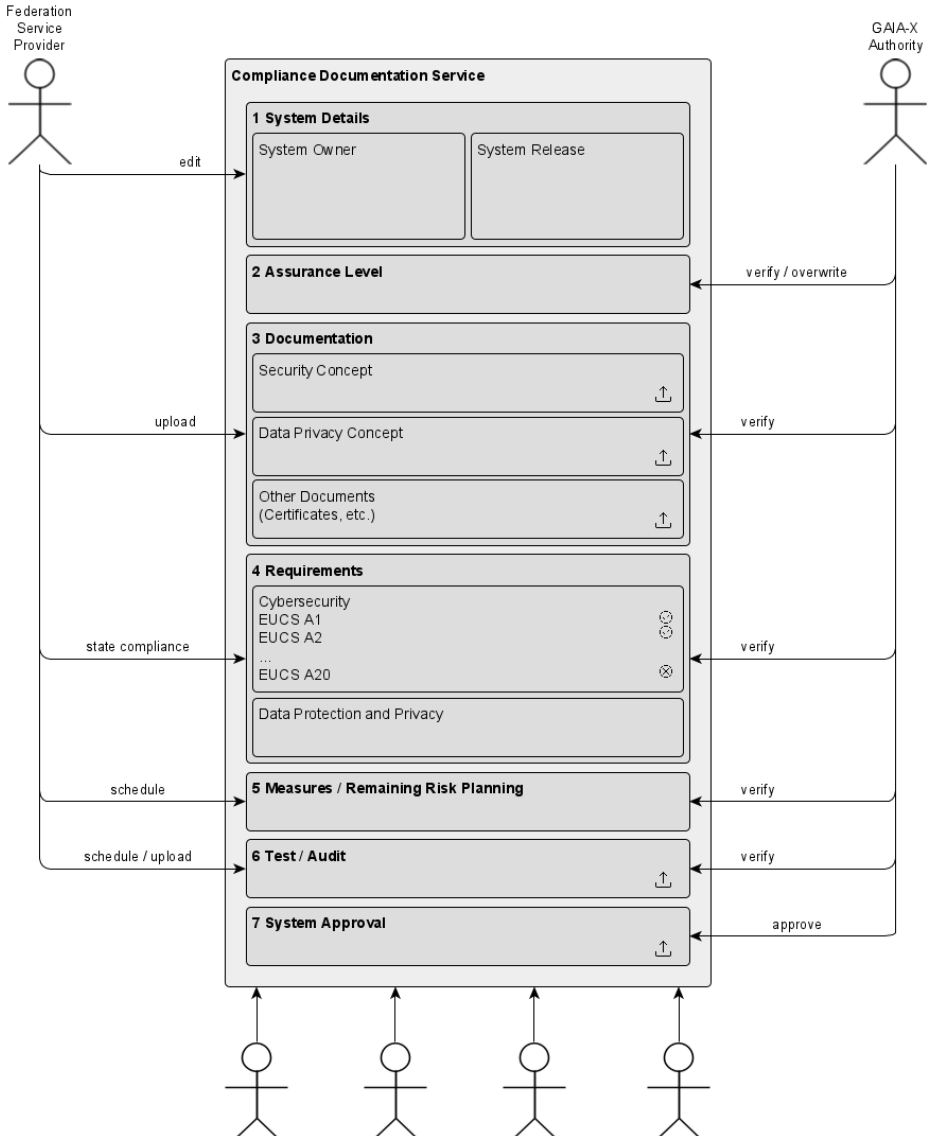

Figure 2: Overview of Compliance Documentation Service

2.1 Product Functions

The main function is the Documentation Service describing the user interaction of the Federation Service Provider and the Gaia-X Authority. The Documentation Service comprises seven functional modules:

- System Details
- Assurance Level
- Documentation
- Requirements and Statements of Compliance
- Measures and Remaining Risk Planning
- Test / Audit
- System Approval

Additionally, the Administration UI is used for the operation, administration, and user support.

2.2 Users Classes and Characteristics

In the following, the minimum roles of the Compliance Documentation Service are briefly described divided into roles for users for the service and roles for operators (operational roles).

User roles

- **System Owner:**
  user role of the Federation Servicer Provider providing compliance information and documents for the Federation Service
- **Approver:**
  user role of the Gaia-X Authority verifying and approving the provided compliance information and documents
- **Auditor:**
  user role having read-only access to all Federation Service systems

Operational roles

- **System Administrator:**
  user role of the Compliance Documentation Service operator managing the system and system data
- **User Administrator:**
  user role of the Compliance Documentation Portal operator managing service and operational users and their permissions
- **Support:**
  supporting user role having read-only access to all Federation Service systems and able to create and process security and data privacy requirements for Federation Services

A restrictive access management is required that ensures the need-to-know principle, e.g., a System Owner is only able to access his system releases.

2.3 Operating Environment

Initially, the Compliance Documentation Service shall be implemented as a stand-alone web service separated from the Gaia-X Federation Services. Besides, it is expected that only few users need access to the service: the Gaia-X Federation Service Providers, the Gaia-X Authority and operators of the service.

A simple realization of the Compliance Documentation Service is to build a typical web application that consists of a web, application and database tier as well as an identity and access management.

Frontend (Web Tier)	- Interacts with service users - Receives data from backend - Acts as security gateway
Backend (Application Tier)	- Contains the application logic - Connected to storage
Storage (Database Tier)	- Stores compliance information of Federation Services - Stores list of cybersecurity and privacy requirements
IAM (Identity and Access Management)	- Management of identities and authentication credentials - Management of users and permissions - Registration and logging on of users

The implementation of the Compliance Documentation Service using Gaia-X Federation Services or components of these is not excluded in principle and may be examined in a later phase of Gaia-X.

2.4 Use Cases

2.4.1 Basic compliance documentation use case

User Registration

A user registers as Federation Service Provider via the Documentation Service UI and is requested to complete his user profile.

System Creation

The registered service provider user creates a new system release for a certain Federation Service by selecting the relevant service type and edits the requested system details. The Gaia-X Authority is notified about the new system release.

User Registration

A user registers as Gaia-X Authority via the Documentation Service UI and is requested to complete his user profile.

Assurance Level Definition

Based on the type of Federation Service, the information about the Assurance Level is predefined in the UI. If necessary, the authority user may overwrite the Assurance Level by selecting another Assurance Level for the system.

Requirement Definition
Based on the Assurance Level and the type of Federation Service, the cybersecurity and privacy requirements are prefilled in the Requirements module of the Documentation Service UI.

User Log On
A user logs on as Federation Service Provider to the Documentation Service UI.

Documentation Provision
The service provider user uploads compliance documents for the Federation Service system, i.e. the security concept, the privacy concept, etc.

Requirement Fulfilment
The service provider user states to each requirement the compliance status, i.e. how the Federation Service system fulfils the requirement.

Action Planning
The service provider schedules mitigating and compensating measures for not fulfilled requirements.

Security Testing
The service provider user uploads security test and audit reports for the Federation Service system.

User Log On
A user logs on as Gaia-X Authority to the Documentation Service UI.

Information Verification
The authority user assesses all provided compliance information (system documentation, Statements of Compliance, security test reports, list of measures and may raise queries to the Service Provider if necessary.

System Approval
The authority user declares (conditional) approval for the Federation Service system by uploading the approval statement to the Documentation Service UI. The Federation Service Provider is notified about the approval.

2.4.2 Further use cases

External Audit
A user (e.g., a governmental regulator) registers as Auditor and receives read access to all Federation Service systems.

Requirement Processing
A user is logged on as support user and edits the security and privacy requirements in the Administration UI.

Support Request

The support is asked by the Federation Service Provider to troubleshoot issues in the operation of the Compliance Documentation Service.

3. System Features

3.1 Documentation Service UI

The Federation Service Provider shall document the deliverables out of the Security and Privacy by Design process in the Documentation Service. The Documentation Service consists of seven service modules where the Service Provider edits information, states compliance, or uploads documents. On the other hand, a Gaia-X Authority is able to read the provided compliance information, verifies, and assesses them. Eventually, an approval statement shall be uploaded.

3.1.1 Module System Details

The first module provides general information about the Gaia-X Federation Service Provider and the corresponding Federation Service. The Service Provider shall enter transparency information about the system owner, system operation and the system release.

The system details are:

- **System Owner**
  - Name of the company
  - Address of the company: street, house number, location, country
  - Contact: name, telephone number, email address
- **System Operation**
  - Name of the company (Operation)
  - Address of the company (Operation)
  - Contact (Operation)
- **System Release**
  - Type of Gaia-X Federation Service
  - Name of the system
  - Release / version of the system
  - Brief description of the system

Documentation Service – System Detail	*Gaia-X Controls Transparency – Criterion*
Name of the company	A.1.1
Address of the company	A.1.1
Contact	A.1.1
Name of the company (Operations)	-
Address of the company (Operations)	-
Contact (Operations)	comparable to A.2.6
Assurance Level of system	-
Name of the system	comparable to A.2.1
Release /version of the system	-
Brief description of the system	comparable to A.2.2

Table 2: Reference of System Details to Gaia-X Transparency Controls criteria

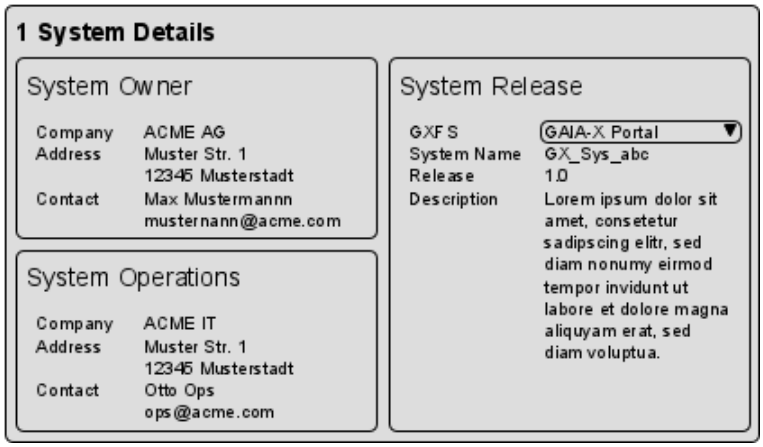

Figure 3: 1st Module System Details – Example

3.1.2 Module Assurance Level of Gaia-X Federation Service

Because of the protection profile analysis ([3] chapter 2), for each Federation Service the Assurance Level was defined. Based on the Assurance Level “basic”, “substantial” or “high”, the Service Provider has to fulfil certain Gaia-X compliance requirements ([3] section 3.4.1).
The type of Federation Service from the System Details module will automatically determine the corresponding Assurance Level. The Gaia-X Authority verifies the selection and, if necessary, may be able to overwrite the Assurance Level.

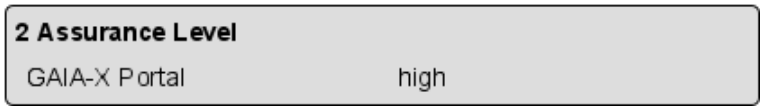

Figure 4: 2nd Module Assurance Level – Example

3.1.3 Module Documentation

In this module any compliance documents, i.e., documents and information that can be used to prove compliance to Gaia-X requirements, shall be uploaded by the Federation Service Provider and verified by the Gaia-X Authority.

Security Concept

The Federation Service Provider shall create a Security Concept that contains the following information:

- [System Description] Documentation of responsibilities
- [System Description] Functional and technical system description
- [Communications Matrices] Overview of internal (between system components) and external connections as well as system management connections.

Source	*Destination*	*Port*	*Protocol*	*Encryption*
User's CLI[2]	System abc's API	443/TCP	HTTPS	yes
System abc	NTP server	123/UDP	NTP	no

Table 3: Example of communication matrix

- [Authorization Concept] Description of (user) roles and functions, e.g. users, administrators, technical users
- [Authorization Concept] Description of user management processes

Data Privacy Concept

The Federation Service Provider shall create a Data Privacy Concept that is the description of the processed PII data of the corresponding Federation Service according to GDPR.

Other compliance documents

Other documents are any documents and information besides the Security and Data Privacy Concept that can used to prove compliance, e.g., ISO 27001 certificate.

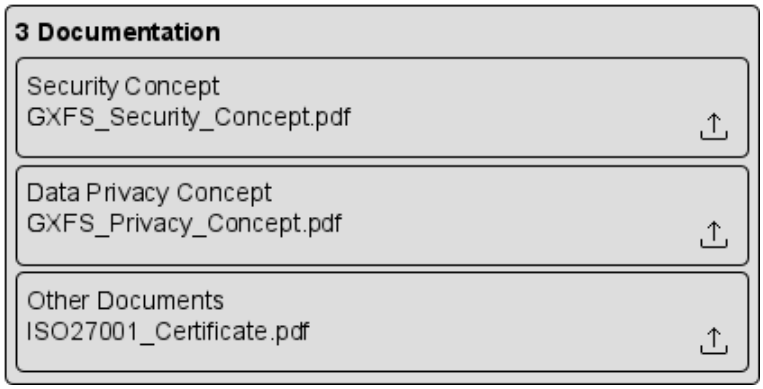

Figure 5: 3rd Module Documentation – Example

3.1.4 Module Requirements and Statement of Compliance

On the one hand, the basic cybersecurity and privacy requirements for the Federation Services are described in [3] section 3.4.1. On the other hand, the Assurance Level determines the level of details how the EUCS (EU Cloud Services Scheme[3]) security controls shall be implemented.

[2] Command Line Interface on user's workstation

[3] https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

Based on the Assurance Level from the second module, the requirements for the Federation Service are automatically pre-filled in the Requirements module. Hence, the Service Provider shall state the compliance to the requirements, i.e., how the provider fulfils the requirements.

Four response options are available:

- Statement of Compliance (SoC): the requirement is fulfilled
- Statement of Partly Compliance (SoPC): the requirement is partly fulfilled
- Statement of Non-Compliance (SoNC): the requirement is not fulfilled
- Statement of Not Applicable (SoNA): the requirement is not relevant

For the response options SoPC, SoNC and SoNA, the Provider shall give reasons for not being fully compliant.

Eventually, the Gaia-X Authority verifies the compliance statements.

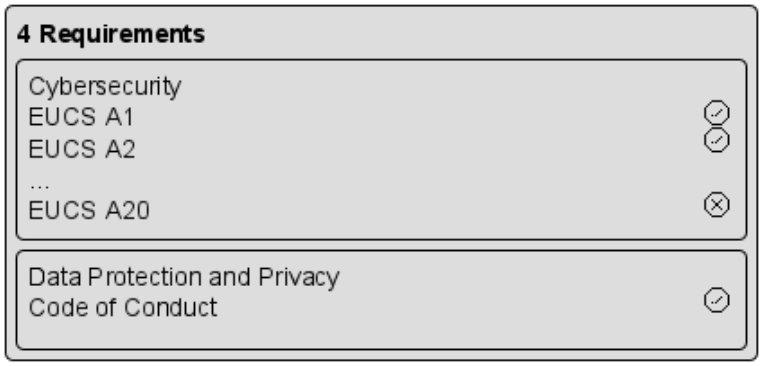

Figure 6: 4th Module Requirements – Example

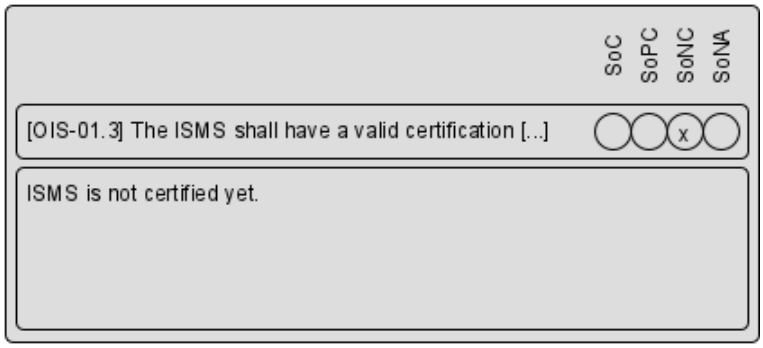

Figure 7: Requirement Response – Example

3.1.5 Module Measures (and Remaining Risk) Planning

In case of not fulfilled requirements from the module Requirements (Statement of Partly Compliance SoPC and Statement of Non-Compliance SoNC), measures to remedy or mitigate the resulting risk shall be defined and scheduled.

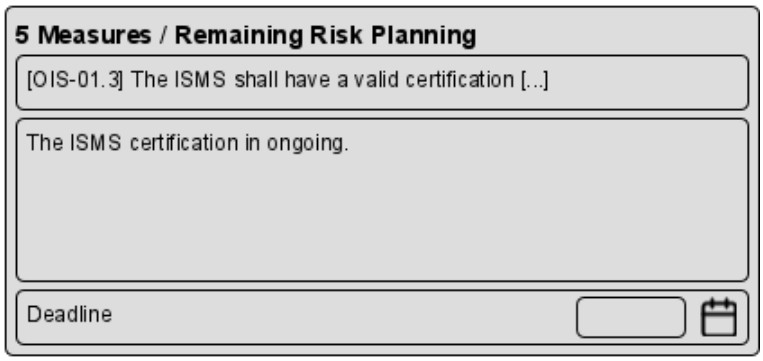

Figure 8: 5th Module Measures - Example

3.1.6 Module Test / Audit

The module Test deals with any topic wrt security testing and audits for Federation Services. The Service Provider shall:

- provide information about performed tests
- upload test and audit reports

The Gaia-X Authority verifies the test and audit reports.

Examples for the security tests during the system's life cycle are described/listed in section 3.4.4 of SPBD [3].

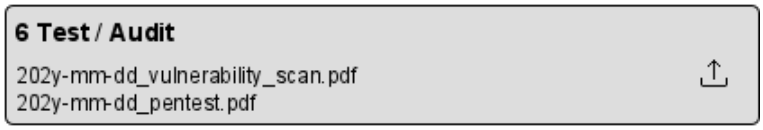

Figure 9: 6th Module Test / Audit – Example

Furthermore, the module may provide interfaces to security and compliance testing tools and procedures in order to make automated and continuous testing possible, e.g., regular vulnerability scans.

3.1.7 Module Approval statement

After the Gaia-X Authority has verified and assessed all necessary system information (e.g., Security Concept, Statements of Compliance, audit reports, etc.), it may declare (conditional) approval for putting the Federation Service into operation or does not approve. The approval statement shall be uploaded.

Figure 10: 7th Module System Approval – Example

3.2 Administration UI

The user interface for service management shall be separated from the user interface of the Documentation Service and shall provide operational and service supporting functions.

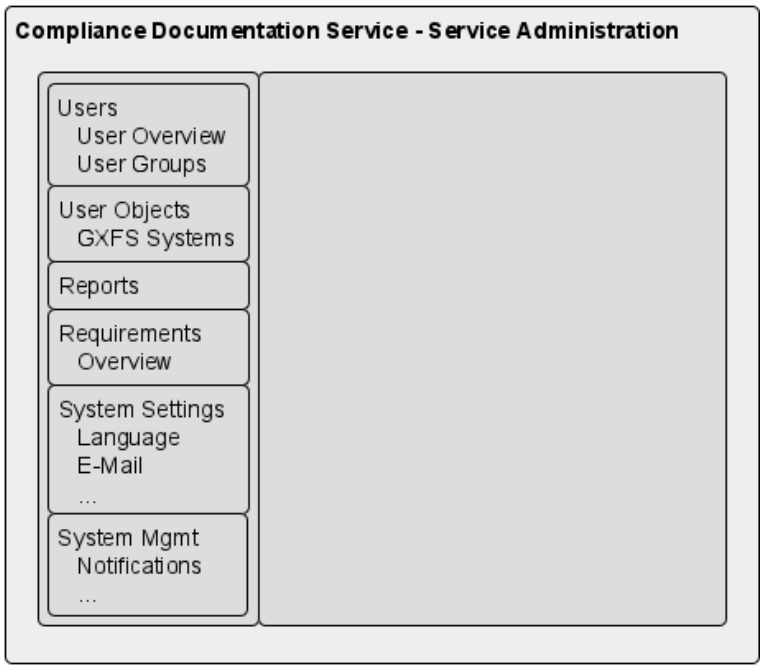

Figure 11: Service Administration Overview – Example

System Administration

System administration includes all tasks to operate, administer and maintain the Compliance Documentation Service, e.g., system configuration.

User Administration

User administrators manage any users and roles of the service and their permissions.

Support Functions

The main functions are the user support, i.e., help users to use the service, and the creation and maintenance of security and privacy requirements.

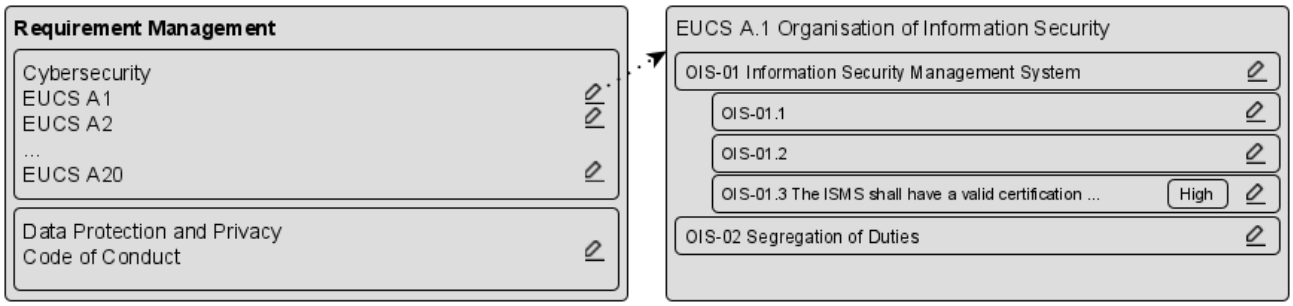

Figure 12: Service Administration Requirement Management – Example

Furthermore, the UI shall provide functionalities to create and export compliance reports for authorized auditors that contains compliance information and approval statements for the Federation Services.

3.3 User Registration

The Compliance Documentation Service includes an identity and access management (IAM) for any users of the service that is necessary for the user registration.

The determining of the authorized participants, especially users acting as service providers, in the Compliance Documentation Service is made by the Gaia-X Authority. It is the result of the tender procedure for the Federation Services. Once a Federation Service Provider has been commissioned, the Service Provider notifies the operator of the Documentation Service of the persons to be authorized. The operator then sets up the corresponding users.

4. Requirements

4.1 Interfaces

4.1.1 Documentation Service UI

Users of the Documentation Service can access the service using a user interface. Initially, the user interface shall be implemented as a web service. For a later phase of Gaia-X, the user interface may be realized with Federation Services or components of these.
Users of the interface are the Federation Service Provider, the Gaia-X Authority and the Auditor.

4.1.2 Administration Interface (user interface, API)

Operational users of the Compliance Documentation Service can access the administration interface via web portal or API. Initially, the interface shall be implemented as a web service. For a later phase of Gaia-X, the interface may be realized with Federation Services or components of these.
Users of the interface are the operational users, i.e., System Administrator, User Administrator and Support. Following the least-privilege principle, users shall have different views on the items of the user interface based on their user role and permissions.

4.1.3 Notification Interface

In order to notify users of the Compliance Documentation Service, the service shall be connected to a notification service (e.g., email service).

4.1.3.1 Testing API(s)

The Compliance Documentation Service may provide an API to integrate external test tools like vulnerability scanners. For example, a user of the web service may initiate a vulnerability check using a connected vulnerability scanner and afterwards the scan report is provided in the Documentation Service UI.

4.1.4 External IAM Interface

The Compliance Documentation Service may connect to an external identity and access management in order to manage the service's users.

4.2 Functional Requirements

Basic functions of the Compliance Documentation Service are described in section 3.

CDS-01	[Usability] The Documentation Service must be simple and intuitive to use. A user must be able to follow the steps of the approval process easily.
CDS-02	[Req Mgmt] Versioning of requirements is required.
CDS-03	[Req Mgmt] Minor and major changes to requirements must be traceable.
CDS-04	[Sys Rel] It must be possible to update the compliance documentation of a Federation Service.
CDS-05	[Sys Rel] When creating a new system release of a Federation Service, it must be possible to take over the existing documentation. Changes to requirements must be taken into consideration.
CDS-06	[Design] The Compliance Documentation Service shall have a modular design. Ideally, the modules may provide interfaces for user interaction.
CDS-07	[Design] The Compliance Documentation Service must be built of Open-Source components.

Table 4: Functional Requirements for Compliance Documentation Service

The list of functional requirements is not exhaustive. Depending on the technical implementation, further requirements shall be defined during the commissioning of the Compliance Documentation Service.

4.3 Non-functional Requirements

4.3.1 General Security Requirements

The Compliance Documentation Service shall fulfil the cybersecurity control set of the EUCS [2] Annex A according to the Assurance Level basic. Further details are given in section 3.4.1 of SPBD specification [3].

4.3.2 Specific Security Requirements

CDS-08	Due to the sensitive compliance information about the Federation Services, the storage of the Compliance Documentation Service must be appropriately encrypted using state-of-the-art mechanisms (data at rest encryption).
CDS-09	Activities of users with privileged access rights (administrative users) shall be logged. (cf. EUCS control IAM-06.2)
CDS-10	The Compliance Documentation Service must be implemented in an audit-proof manner.

Table 5: Specific Security Requirements for Compliance Documentation Service

The list of specific security requirements is not exhaustive. Depending on the technical implementation, further requirements shall be defined during the commissioning of the Compliance Documentation Service.

4.3.3 Data Protection and Privacy Requirements

The Compliance Documentation Service must be compliant with GDPR; see section 3.4.1 of SPBD specification [3] and [4].

4.3.4 Other non-functional Requirements

CDS-11	The system shall fulfil accessibility and ergonomics requirements.

Table 6: Other non-functional Requirements for Compliance Documentation Service

Appendix A: Glossary

The glossary is part of the Gaia-X Architecture Document [1].

Appendix B: Overview GXFS Work Packages

The project "Gaia-X Federation Services" (GXFS) is an initiative funded by the German Federal Ministry of Economic Affairs and Energy (BMWi) to develop the first set of Gaia-X Federation Services, which form the technical basis for the operational implementation of Gaia-X.

The project is structured in five Working Groups, focusing on different functional areas as follows:

Work Package 1 (WP1): Identity & Trust
Identity &Trust covers authentication and authorization, credential management, decentral Identity management as well as the verification of analogue credentials.

Work Package 2 (WP2): Federated Catalogue
The Federated Catalogue constitutes the central repository for Gaia-X Self-Descriptions to enable the discovery and selection of Providers and their Service Offerings. The Self-Description as expression of properties and Claims of Participants and Assets represents a key element for transparency and trust in Gaia-X.

Work Package 3 (WP3): Sovereign Data Exchange
Data Sovereignty Services enable the sovereign data exchange of Participants by providing a Data Agreement Service and a Data Logging Service to enable the enforcement of Policies. Further, usage constraints for data exchange can be expressed by Provider Policies as part of the Self-Description

Work Package 4 (WP4): Compliance
Compliance includes mechanisms to ensure a Participant's adherence to the Policy Rules in areas such as security, privacy transparency and interoperability during onboarding and service delivery.

Work Package 5 (WP5): Portal & Integration
Gaia-X Portals and API will support onboarding and Accreditation of Participants, demonstrate service discovery, orchestration, and provisioning of sample services.

All together the deliverables of the first GXFS project phase are specifications for 17 lots, that will be awarded in EU-wide tenders:

Further general information on the Federation Services can be found in [1].

Appendix C: Archimate Model

Compliance Documentation Service