3DxVERSE

Work Package 5

D5.1: Security and Privacy of Digital Twins - First Report

ww.3DxVERSE.eu

3DxVERSE project is co-funded by the European Union's Digital Europe Programme (DIGITAL) under grant agreement No. 101168258.

History of changes

Work Package	WP5
Task 3.1	Security and Privacy of Digital Twins-First Report
Authors	Harm Arendshorst ILABS Nicky Hickman ILABS
Dissemination Level	Public
Status	Final
Due date	31/05/2025
Document Date	30/05/2025
Version Number	1.0

Quality Control

	Name	Organisation	Date
Editor	Harm Arendshorst	ILABS	05/05/2025
Peer review 1	Ralf Willenbrock	ERTICO	12/05/2025
Peer review 2	Helmut ten Have	Adecs	19/05/2025
Authorised by (Technical Coordinator)	Harm Arendshorst	ILABS	23/05/2025
Authorised by (Quality Manager)	Lampros Stergioulas	HUAS	26/05/2025
Submitted by (Project Coordinator)	Dr. Eusebiu Catana	ERTICO	30/05/2025

Legal Disclaimer

3DxVERSE is co-funded by the European Commission, Digital Europe programme under grant agreement No. 101168258 (Digital). The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The 3DxVERSE Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

TABLE OF CONTENTS

History of changes 2
Quality Control 2
Legal Disclaimer 2
List of abbreviations and acronyms 6
Executive Summary 7

1. INTRODUCTION 9
1.1. Introduction to 3DxVERSE 9
1.2. Vision: A Globally Scalable, Citizen-Centric Digital Twin Ecosystem for Sustainable Living and Travel 9
1.3. Purpose of the deliverable 10
1.4. Intended audience 12
1.5. Status of the deliverable 12

2. STATE OF THE ART REFERENCE IMPLEMENTATION OF INTEROPERABLE DIGITAL TWINS 13
2.1. What is a Reference Implementation and a Testbed? 13
2.2. How will be done? 13

3. DRAFT DIGITAL TWIN AND AI TRUST FRAMEWORK 15
3.1. What is a Trust Framework? 15
3.2. Introduction 15
3.3. Methodology and Approach 17
3.4. Language and Terminology 17
3.5. Purpose 17
3.6. Scope (who and what the Trust Framework applies to) 17
3.7. Objectives (what the Trust Framework achieves) 19
3.8. Principles (the values underpinning the Trust Framework) 19
3.9. General Requirements (what the primary rules of the Trust Framework are) 21
3.10. Schedule of Controlled Documents 22
3.11. Change Control (how to revise the Trust Framework) 23

4. DRAFT DEVSECOPS FRAMEWORK 24
4.1. What is a Dev Sec Ops Framework? 24
4.2. DevSecOps Framework and Toolchain 24
4.3. Conformity Assessment and Certification 26
4.4. Risk Management Framework 27
4.5. Dual Use of Digital Twins: Enabling Resilience, Security & Strategic Readiness 29
4.6. Analysis of Trust Lists and Trust Registries 30

5. PRIVACY, SECURITY AND VALUE CREATION BY DESIGN 31
5.1. Socio-Technical Systems Design in Practice 31
5.2. Proposed Timeline of Iterations for Use Cases 32
5.3. Adaptive, Machine Enforceable Governance 33
5.4. Technology: Agile Development and Backlog 34
5.5. Product KPI's as Prioritisation Criteria 35
5.6. Practical recommendations for ecosystem participants in WP6 (Use Cases) and WP8 (Pilots and Citizen Engagement) 35

6. CONCLUSIONS – 3DXVERSE AT THE FRONTIER OF TRUSTWORTHY DIGITAL TWINS 37

7. ANNEXES 39
7.1. EU Legislative Requirements 39
7.2. Disaster Recovery & Business Continuity Plan 40
7.3. Interoperability Testbed (ITB) for Interoperability Testing and Validation 41
7.4. EU & Global Standards alignment 42
7.5. Trust Lists and Trust Registries 47
7.6. Detailed roles and responsibilities in 3DxVERSE 48
7.7. Detailed Functions as User Stories mapped to EU legislation and standards 49
7.8. Trust Frameworks Controlled Documents 54

REFERENCES 59

LIST OF FIGURES

Figure 1: Cartoon illustration of sustainable travel use case. Image generated by ChatGPT (09/05/25). 10
Figure 2: Logical view of the interdependencies between Work Packages in the 3DxVERSE project. 11
Figure 3: Illustration of interdependencies between this deliverable D5.1 and tasks and deliverables in other work packages, and how this will be tested in deliverable D5.2. 11
Figure 4: EU Digital Rights & Principles (Source: https://hei-prometheus.eu/) 16
Figure 5: The Trust over IP Model (Source: Trust over IP Foundation) 17
Figure 6: Overview of the scope of functions that the Trust Framework must support (image generated by Napkin.ai) 19
Figure 7: Illustration of the Facets of Trustworthiness. (Image generated by Napkin.ai; derived from Maple et al., 2021 Ref 2) 21
Figure 8: Illustration of DevSecOps Agile Process (Source: https://www.plutora.com/blog/devsecops-guide) 24
Figure 9: Interoperable EU Risk Management Toolbox Process (Source: ENISA) 27
Figure 10: The New European Bauhaus Compass - Participatory Process, Transdisciplinary approach and Multi-Level Engagement (Source: NEB Toolbox, Ref 10) 31
Figure 11: Illustration of the per use case iteration showing social design, governance and technology 32
Figure 12: Snapshot of the high-level implementation plan showing use case iterations against a timeline of releases 33
Figure 13: Illustration of the process by which Trust Framework is developed and operated for adaptive, machine enforceable governance 34
Figure 14: OASC MIMs Plus Conformance Testing 42

LIST OF TABLES

Table 1: Privacy Standards Alignment 43
Table 2: Cybersecurity Standards Alignment 43
Table 3: Physical and IoT Security Standards 44
Table 4: Interoperability Standards 45
Table 5: Environmental Security Standards 46
Table 6: Trust Lists and Trust Registries Analysis 47
Table 7: Provider Roles and Responsibilities 48
Table 8: Consumer Roles and Responsibilities 49
Table 9: Observer Roles and Responsibilities 49
Table 10: Detailed Functions as User Stories 50
Table 11: Status against the ENISA Risk Management Process 54

List of abbreviations and acronyms

Abbreviation	Meaning
ABAC	Attribute-Based Access Control
AI	Artificial Intelligence
DevSecOps	Development Security Operations
DGA	Data Governance Act
DSA	Digital Services Act
EC	European Certification
eIDAS	European Identity, Authentication and trust Services
EIF	European Interoperability Framework
EIRA	European Interoperability Reference Architecture
ETSR	Ethical Trade and Social Responsibility
EU	European Union
FIDO	Fast Identity Online
GDPR	General Data Protection Regulation
IATA	International Air Transport Association
ICT	Information and Communication Technology
IDSA	International Data Spaces Association
ISO	International Organization for Standardization
ITB	Interoperability Testbed
ITU	International Telecommunication Union
MIMs	Minimum Interoperability Mechanisms
NIS2	Network and Information Security Directive 2
OASC	Open and Agile Smart Cities
OWASP	The Open Worldwide Application Security Project
RBAC	Role-Based Access Control
SD-JWT	Selective Disclosure - JSON Web Token (A form of Verifiable Credential)
SOTA	State Of The Art
TEE	Trusted Execution Environment
TF	Trust Framework
VC	Verifiable Credential

EXECUTIVE SUMMARY

The **3DxVERSE project** pioneers the creation of a globally scalable, interoperable, and citizen-centric **Digital Twin ecosystem** to foster sustainable living and mobility. This deliverable—**D5.1: Security and Privacy of Digital Twins: First Report**—establishes the **technical, legal, and ethical foundations** for building **trusted, secure, and interoperable digital twin infrastructures** across multiple sectors.

This report defines a strategic blueprint for systematically embedding **trust, privacy, and security** throughout the lifecycle of Digital Twin implementations. It provides actionable guidance for **operational teams**, **governance entities**, and **project stakeholders**, ensuring compliance, resilience, and alignment with European values and legal frameworks.

The deliverable introduces three interdependent frameworks:

Digital Twin and AI Trust Framework: Governs access, usage, and accountability within digital and AI-driven systems.

DevSecOps Implementation Framework: Integrates security measures across agile software development cycles.

Socio-Technical Design Model: Promotes participatory, ethical, and inclusive design principles.

These frameworks are aligned with evolving European legislation—**NIS2 Directive**, **AI Act**, **Data Governance Act**—and international standards to ensure **interoperability**, **rights-based innovation**, and **machine-enforceable compliance**. The approach supports **dual-use contexts** (civilian and defence), robust algorithmic governance, and secure data sharing.

Chapter 1: Introduction

Introduces the vision of 3DxVERSE as a global model for citizen-centric digital twin development, grounded in the **New European Bauhaus** principles of sustainability, aesthetics, and inclusiveness. It outlines the deliverable's role within the broader project and its integration with key work packages (WP3, WP4, WP5, WP6).

Chapter 2: State of the Art Reference Implementation

Describes the first implementation of the **Interoperable Digital Twin Testbed**, designed in WP3 and operationalised in WP7. It clarifies the distinction between reference architecture and testbed and highlights integration efforts with **eIDAS 2.0**, **ESRI platforms**, and collaborative activities with **iLabs**, **IATA**, and the **European Commission's Interoperability Testbed**.

Chapter 3: Draft Digital Twin and AI Trust Framework

Outlines a comprehensive **Trust Framework**, comprising rules, roles, and mechanisms for secure, ethical, and compliant exchanges of data and digital identity. Grounded in GDPR, the AI Act, and NIS2, and aligned with **Trust over IP** models, it includes governance roles, document control systems, and change management strategies to enable **machine-enforceable trust** across domains and jurisdictions.

Chapter 4: Draft DevSecOps Framework

Details the technical implementation of trust and security using a **DevSecOps approach** across the **Software Development Life Cycle (SDLC)**. It integrates ENISA-aligned risk management, addresses **dual-use implications**, and evaluates **trust infrastructures** such as **OpenID Federations** and **blockchain-based trust registries**.

Chapter 5: Privacy, Security and Value Creation by Design

Emphasises the embedding of privacy and security through **participatory and agile development**. Drawing on **socio-technical systems theory** and the **New European Bauhaus Compass**, this chapter presents methods to align social equity with technological development. It includes practical tools, KPIs, and design guidelines for WP6, WP7, and WP8 to ensure trust, inclusion, and measurable public value.

Designed as a practical guide, this deliverable equips partners in WP6 (Use Case Design), WP7 (Technical Implementation), and WP8 (Pilots & Citizen Engagement) with actionable tools, policies, and standards to ensure that 3DxVERSE delivers trustworthy, inclusive, and secure digital public infrastructure. By embedding societal values into its architecture and development process, 3DxVERSE emerges as a European flagship for human-centric digital transformation.

Chapter 6: Conclusions

Designed as a practical and strategic resource, this deliverable equips project partners—particularly those engaged in use case design (WP6), technical implementation (WP7), and citizen engagement (WP8)—with the frameworks and tools required to implement **trusted, inclusive, and secure digital infrastructures**.
By embedding **European values** and **societal priorities** into both architecture and operations, the 3DxVERSE project positions itself as a **flagship initiative** for **human-centric digital transformation**. It sets a precedent for the responsible deployment of Digital Twins in line with ethical standards, legal compliance, and future-oriented technological leadership.

1. INTRODUCTION

1.1. Introduction to 3DxVERSE

The 3DxVERSE project aims to harness the potential of Digital Twins to foster sustainable travel and living communities. The initiative focuses on key use cases at various levels, from airports to living communities, encompassing sustainability, economic growth, societal development, safety, security, resilience, and corporate sustainability responsibility in a holistic approach. By establishing interoperable Digital Twins and leveraging cutting-edge technologies like AI, XR/VR and Data Spaces, this project aligns with the New European Bauhaus initiative and the G20 Framework for Systems of Digital Public Infrastructure.

Through potential collaboration with organisations like the International Data Spaces Association, Open & Agile Smart Cities (OASC) working on the OASC Minimal Interoperability Mechanisms (MIMs), and European Digital Infrastructure Consortia (EDIC's), we seek to create a transformative impact on digital inclusion, innovation, and sustainability, contributing to the achievement of the 2030 Agenda for Sustainable Development.

By creating an open, interoperable, secure, trustworthy, fair and inclusive reference implementation blueprint Digital Twin for EU citizens, businesses and public administrations, this project strives to build a resilient, inclusive, and environmentally conscious digital economy and society.

The focus on societal impact, economic growth, and sustainability reflects our commitment to achieving the Sustainable Development Goals and shaping Europe's digital future. The project involves collaboration with global partners, including Amsterdam, Rotterdam, Almelo, Enschede, Aruba, Hamburg and can scale to global collaboration with partner countries, including Africa, India, Singapore, Japan, UK, and Canada.

1.2. Vision: A Globally Scalable, Citizen-Centric Digital Twin Ecosystem for Sustainable Living and Travel

3DxVERSE envisions a globally available digital twin infrastructure that empowers citizens, governments, and service providers—public and private alike—to collaboratively shape more sustainable, inclusive, and resilient societies.

What makes 3DxVERSE truly unique is its grounding in a Participatory Design and Digital Commons approach, ensuring that digital twin technologies are co-created with and for the communities they serve. This foundation ensures that trust, transparency, and accessibility are built in from day one.

3DxVERSE architecture supports real-time governance operations alongside modern DevSecOps methodologies, seamlessly integrating operational intelligence with continuous development, security, and compliance pipelines.

By addressing the fragmentation of trust frameworks and the complexity of regulatory compliance across jurisdictions, 3DxVERSE provides a unifying backbone for interoperable, cross-sector digital twins.

We embrace the evolution of international standards, supporting both physical and digital twins—and more importantly, how they interact with one another in dynamic, real-world environments.

At its core, 3DxVERSE bridges the gap between data exchange, AI-driven insights, and value exchange mechanisms (like digital identity, payments, and CO_2 offsetting), unlocking new modes of engagement between humans, machines, and environments.

Whether optimizing travel emissions, enhancing urban mobility, or supporting clean energy transitions, 3DxVERSE stands for a new generation of human-centric digital infrastructure—scalable, secure, and sustainable.

The cartoon below illustrates a traveller use case to Aruba and demonstrates how 3DxVERSE supports citizen engagement and delivers real-world experiences.

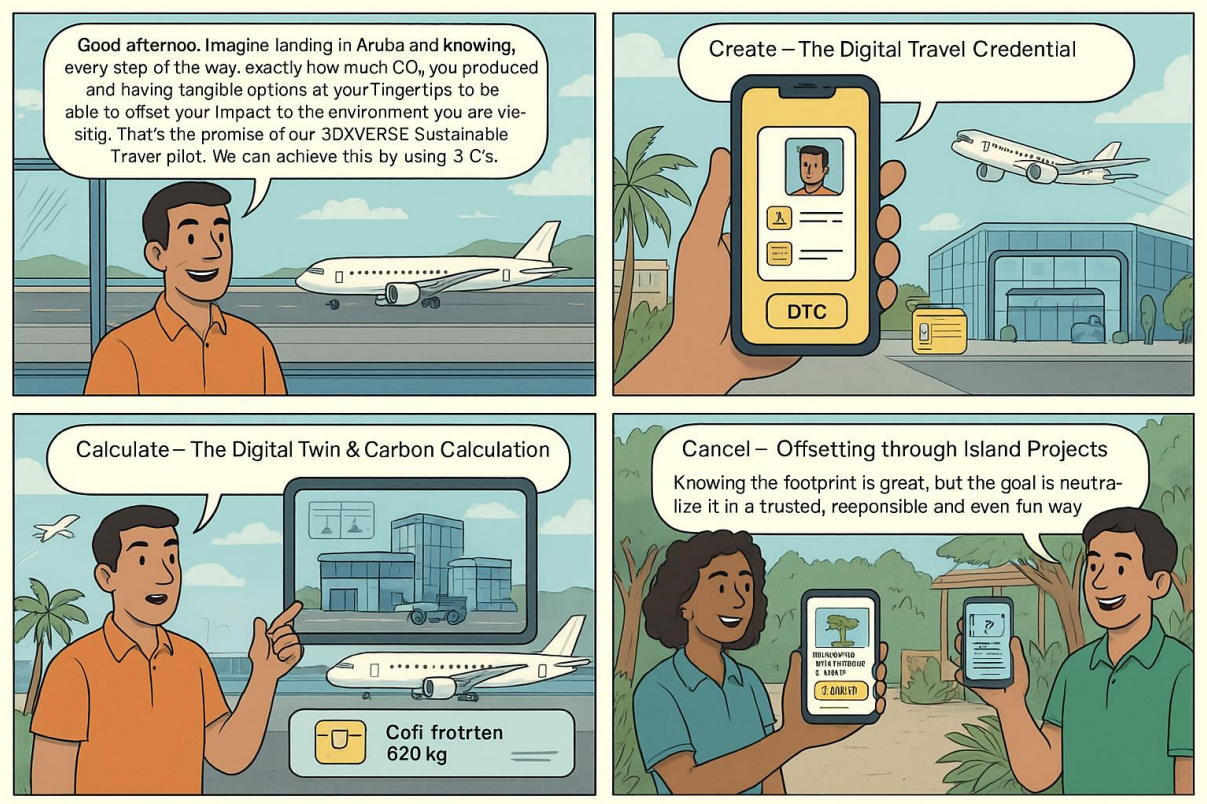

Figure 1: Cartoon illustration of sustainable travel use case. Image generated by ChatGPT (09/05/25)

1.3. Purpose of the deliverable

This Security and Privacy Report of 3DxVERSE is delivered as part of WP5 (Security & Privacy of Digital Twins). WP5 focuses on developing a Digital Twin and AI Trust Framework, led by iLabs. This framework incorporates European regulations on cybersecurity, ethical AI, digital identity, and data protection. It aligns with Digital Principles and New Bauhaus Principles to create an inclusive, secure, and interoperable digital twin platform. The objective is to deliver a best-practice reference implementation.

WP5 will assure the main input from: WP3 – Digital Twin Interoperability Testbed and Reference Architecture. WP3, WP4 and WP5 will assure the backbone of the WP6- Use case Design, to design and develop the Use Cases for Sus-tainable Travel and Living Communities. They will design versatile and effective digital twins for sustainable living communities, smart mobility hubs and airports, ensuring their seamless integration and positive societal impact. This work package aims to deliver well-defined, impactful digital twin implementations through data modelling, scenario planning, simulation, integration of advanced technologies, and thorough evaluation using predefined impact metrics.

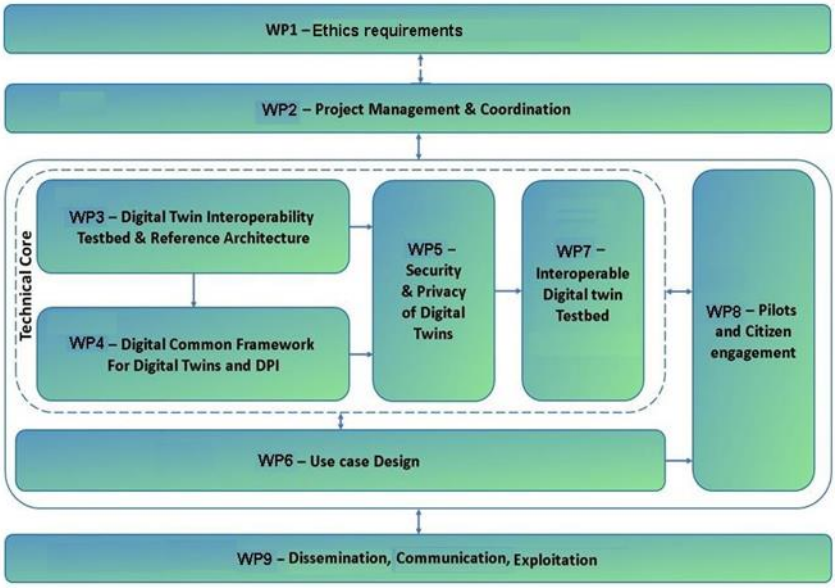

Figure 2: Logical view of the interdependencies between Work Packages in the 3DxVERSE project

The purpose of this deliverable is to build on the requirements from upstream Work Packages (D1.1 Ethics Requirements; D2.2 Data Management Requirements; D3.1 Technical Requirements; D4.1 Digital Commons Principles and Governance Requirements and initial Business Requirements from D6.1 Use Case Design) on which we are dependent, and provide implementation designs and guidance for dependent Work Packages (WP6 Use Case Design, WP7 Interoperable Digital Twin Testbed, and WP8 Pilots & Citizen Engagement) . These interdependencies are illustrated below.

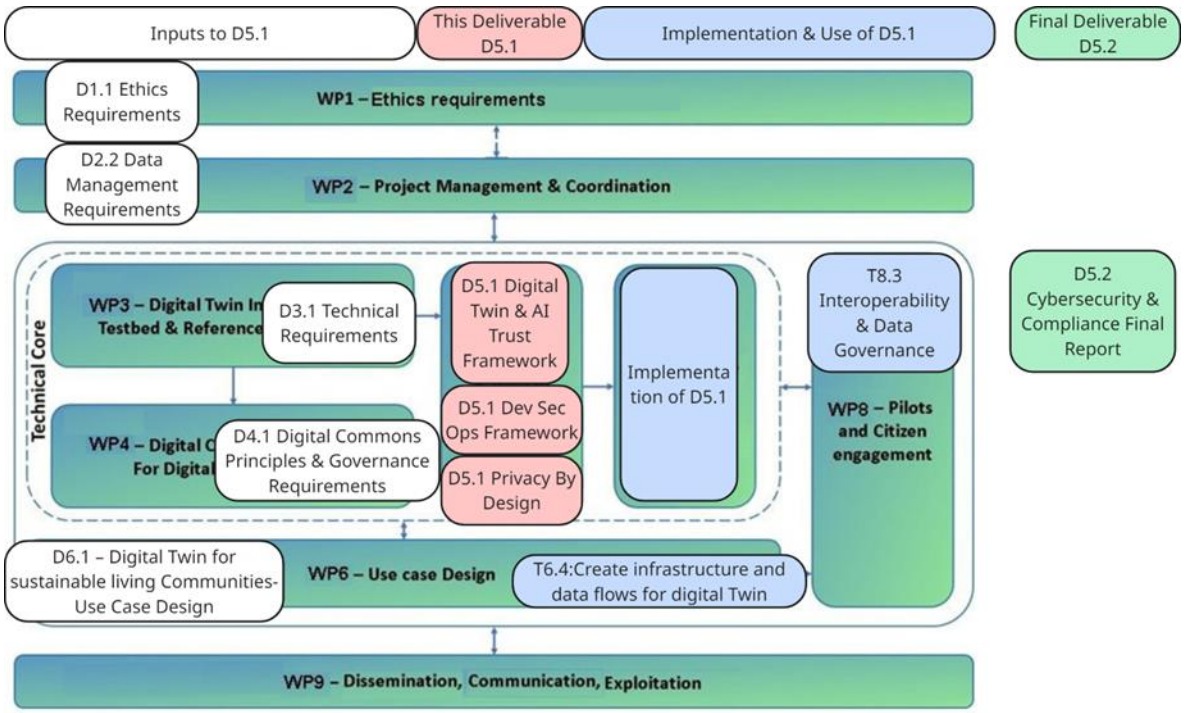

Figure 3: Illustration of interdependencies between this deliverable D5.1 and tasks and deliverables in other work packages, and how this will be tested in deliverable D5.2.

This deliverable 5.1 Security & Privacy of Digital Twins First Report provides updates against each of the tasks in the WP.

- **T1** *Draft* **Digital Twins and AI Trust Framework**: The policies, processes and compliance standards for the access and use of interoperable digital twin ecosystems for sustainable living and mobility in WP4 (Digital Commons), WP6 (Use Case Design), WP 7 (Interoperable Digital Twin Test Bed) and WP8 (Pilots and Citizen Engagement).
- **T2** *Draft* **Dev SecOps Framework**: How those policies, processes and compliance standards are implemented, maintained and assured in WP7 (Interoperable Digital Twin Testbed) and WP8 (Pilots and Citizen Engagement).
- **T3** *Recommended* **Security, Privacy and Value Creation** By Design: Processes for WP 6 (Use Case Design), specifically T6.4 Create Infrastructure and data flows for digital Twin, WP7 (Interoperable Digital Twin Testbed) and WP8 (Pilots and Citizen Engagement), specifically T8.3 Interoperability & Data Governance.
- **T4** *Designing* **Security & Privacy of Digital Twins**: How we develop and use the security and privacy capabilities for 3DxVERSE over the lifetime of the programme, and how this is used by different participants.

A second deliverable 5.2 Cybersecurity & Compliance Final Report, due in May 2027, will contain:

- **T1** *V1* **Digital Twins and AI Trust Framework** and a compliance report.
- **T2** *V1* **Dev SecOps Framework** and a compliance report.
- **T3** *Implemented* **Security, Privacy and Value Creation By Design** Processes with a compliance report on their implementation in WP 6 (Use Case Design), specifically T6.4 Create Infrastructure and data flows for digital Twin, WP7 (Interoperable Digital Twin Testbed) and WP8 (Pilots and Citizen Engagement), specifically T8.3 Interoperability & Data Governance.
- **T4** *Testing* **Security & Privacy of Digital Twins**: for protection and resistance to cybersecurity attacks and prevention of privacy breaches.

By complying with the Trust Framework, organizations, individuals and things can confidently and reliably connect, interact or transact, ensuring privacy, security, accessibility and usability for all parties both internal to the 3DxVERSE ecosystem and external parties interacting or transacting with interoperable Digital Twin implementations.

1.4. Intended audience

The dissemination level of D5.1 is ‘Public’ (PUB) and it is available to the members of the consortium, the European Commission (EC) services and those external to the project.

This document is primarily intended to serve as an internal guideline and reference for all 3DxVERSE beneficiaries, especially the governance bodies such as the General Assembly, the Steering Committee, the Technical Management Team, and the Advisory Board.

1.5. Status of the deliverable

The information used in the deliverable and the situation description of the project management procedures is based on the consortium and project plan situation in May 2025.

WP3 will assure the main input to: WP4 – Digital Common Framework and WP5 – Security & Privacy of Digital Twins and WP7 Interoperable Digital Twin Testbed. WP3, WP4 and WP5 will assure the backbone of the WP6- Use case Design» design and develop the Use Cases for Living Communities and Sustainable Travel. They will design versatile and effective Digital Twins for sustainable living communities and airports, ensuring their seamless integration and positive societal impact.

2. STATE OF THE ART REFERENCE IMPLEMENTATION OF INTEROPERABLE DIGITAL TWINS

Essential for delivering the 3DxVERSE objectives is a reference implementation and testbed designed in WP3 (Digital Twin Interoperability Testbed and Reference Architecture) and implemented in WP7 (Interoperable Digital Twin Testbed). This chapter outlines the status of this implementation and the essential integrations that will be made over the course of the programme.

2.1. What is a Reference Implementation and a Testbed?

A **reference architecture** is a strategic blueprint that outlines how different parts of a digital system (such as soft-ware, data, and infrastructure) should be structured and work together. The reference architecture is a design tem-plate that guides the development of technology solutions—ensuring consistency, interoperability, and alignment with business goals. This best-practice framework helps organisations build faster, reduce risk, and stay future-proof.

A **testbed** is a controlled, real-world environment where new digital technologies, systems, or services can be safely tested, validated, and improved before full-scale deployment. It functions like a proving ground or innovation lab, allowing companies and governments to experiment with cutting-edge solutions (like AI, IoT, or smart data platforms) to see what works, understand the impact, and de-risk investments.

The technical requirements for 3DxVERSE are specified in D3.1 (Digital Twin Interoperability Testbed and Reference Architecture First Report). The governance requirements are specified in this deliverable 5.1 Chapter 3 DRAFT Digital Twin and AI Trust Framework. They are implemented in WP7 (Interoperable Digital Twin Testbed).

Already delivered for use in the 3DxVERSE project and supplied by ESRI is a reference implementation of Interoperable Digital Twins. The detailed architecture is contained in D3.1 Digital Twin Testbed and Reference Architecture. ESRI employ a comprehensive DevSecOps Framework based on OWASP (Open Web Application Security Project) and have key conformance certifications detailed below. The 3DxVERSE implementation will interconnect at EU and then global scale to provide sustainable and interoperable digital twin capabilities for citizens, public and private sector use. You can see ESRI's impressive capabilities here https://www.esri.com/en-us/digital-twin/overview.

2.2. How will be done?

Over the course of the programme 3DxVERSE will integrate other interoperability services in development.

- eIDAS 2.0 (European Identity, Authentication and Trust Services) Interoperability Testbed and Interoperable Europe Test Suite
- iLabs has been working together with the European Commission Interoperability Testbed (ITB) team to develop an specific interop test service for Verifiable Credentials and biometric onboarding (for the Airport Technology Lab Testbed). iLabs also organized a hackathon (8 and 9 June 2023) to develop and test the new specification for Selective Disclosure and Verifiable Credentials based on SD-JWT.
- iLabs has been working together with the OpenID Test Suite team to develop a test case for this recent specification and VC (Verifiable Credential) profile now brought under the Linux Foundation - Open Wallet Foundation.

- iLabs is working together with the IDSA (International Data Space Association) on the specification and implementation of a Digital Identity Connector as part of the open-source Eclipse project that will be based on privacy by design principles.

- iLabs is also working in the Netherlands on a Decentralized Identity profile and testbed together with the Dutch BlockChain Coalition, Dutch Future Mobility Alliance, and the associated organizations working on a Decentralized Digital Identity Testbed, including banks, tax office, chamber of commerce working on a Company Passport (Company Wallet).

- iLabs is also working together with IATA (International Air Travel Association) on Business Credentials and Traveller Identity specifications based on Verifiable Credentials.

Based on this work 3DxVERSE will be able to leverage latest developments to accelerate the development and implementation of a Decentralized Digital Identity model for Digital Twins, based on W3C Open Standards. This capability enables access control (identification, authentication and authorization) of all entities (people, organizations and things) as well as enriched data sharing capabilities across jurisdictions promoting interoperability. Details of the implementation are in Annexe Interoperability Testbed (ITB) for Interoperability Testing and Validation.

To support the technical implementation in the next chapter we turn to the governance mechanisms and rules that will determine how that technical implementation is used, by whom and under what conditions.

3. DRAFT DIGITAL TWIN AND AI TRUST FRAMEWORK

This chapter creates a *Draft* **Digital Twin and AI Trust Framework**: The policies, processes and compliance standards for the access and use of interoperable digital twin ecosystems for sustainable living and mobility in WP4 (Digital Commons), WP6 (Use Case Design), WP 7 (Interoperable Digital Twin Test Bed) and WP8 (Pilots and Citizen Engagement).

3.1. What is a Trust Framework?

A trust framework (also known as a governance framework) is a **structured set of rules, policies, processes and standards**, that enables parties to confidently share and rely on identity, data or services in a consistent, secure, and interoperable way.

In simple terms, it's a **governance model** that defines:

- **Who and what is trusted** (i.e. people, organizations, and both physical and logical things)
- **For what purpose** (e.g. sharing identity data, accessing services)
- **Under what conditions** (e.g. authentication levels, privacy requirements)
- **With what assurance** (e.g. certification, verification, audit)

A trust framework is crucial for establishing and maintaining trust among different entities in digital interactions, ensur-ing compliance, and facilitating secure and reliable transactions and interactions.

3.2. Introduction

The Digital Twin and AI Trust Framework focuses on security, privacy, resilience and interoperability in line with EU priorities and is grounded in EU Digital Rights and Principles (see below) and reflects the New Bauhaus principles of sustainability, inclusion and aesthetics (Chapter 5 Privacy, Security and Value Creation by Design).

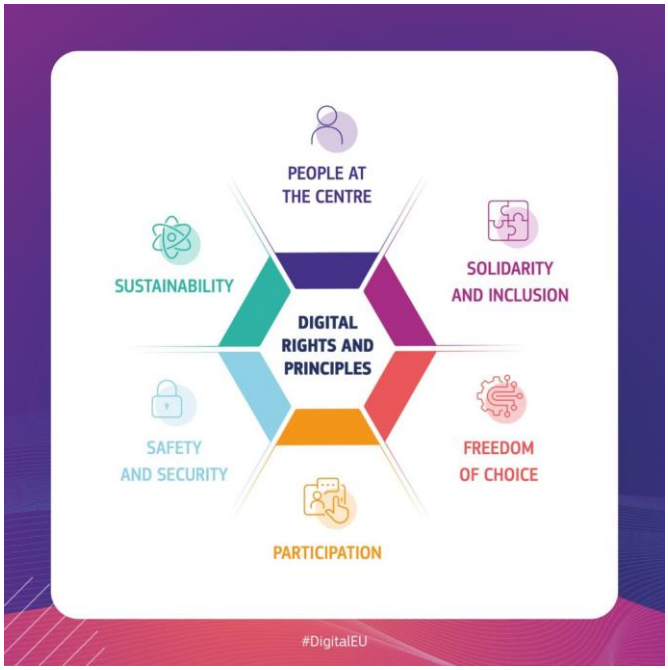

Figure 4: EU Digital Rights & Principles (Source: https://hei-prometheus.eu/)

The Trust Framework derives its rules, policies, processes and standards from the existing and emerging European regulations which collectively aim to create a digital environment that is inclusive, secure, trusted, resilient, sustainable, open, safe, and interoperable. They promote inclusive access to digital services and identity (eID Framework, DSA), safeguard fundamental rights and data privacy (GDPR, AI Act), and build public trust through transparency, accountability, and ethical use of AI and digital technologies. Security and resilience are reinforced through comprehensive cybersecurity measures (Cybersecurity Regulation, NIS2, Cyber Resilience Act, Cyber Solidarity Act), while the sustainability and openness of the digital economy are supported by fair data access and innovation-friendly rules (Data Governance Act). Interoperability across borders and systems is ensured through common standards and public sector collaboration (Interoperable Europe Act), enabling a cohesive and human-centred digital transformation across the EU that will unleash the potential of the digital economy.1

Security and privacy are cornerstones of trustworthiness, but they are not the whole picture. We must add resiliency, robustness, ethics and reliability.[2]

The Trust Framework builds on the Ethics of CitiVerse (ETSR)3 which have already derived their rules from applicable EU regulations focused on the ethical, legal, and human rights implications of data use, technology deployment, and participation in smart city initiatives (e.g., privacy, consent, fairness, accessibility). 3DxVERSE will extend these further to enable the practical implementation of technologies and services to improve urban living and emphasizes efficiency, innovation, and service delivery in the use by human participants of their personal data, and technologies. The 3DxVERSE Digital Twin and AI Trust Framework will therefore emphasize value creation for all participants, and interoperability.

We will leverage and interoperate with existing Trust Frameworks and standards (See Annexe EU and Global Standards Alignment), to create a scalable Trust Framework for trustworthy sharing of data, algorithms and services across all partner countries and sectors.

3.3. Methodology and Approach

The Trust Framework (also known as a governance framework) is aligned with the Trust over IP Foundation (Governance) MetaModel for structural purposes which recognises that governance sits alongside technology in a twin stack and is **a functional, adaptive method of risk management** underpinned by a dynamic, iterative and participatory process.

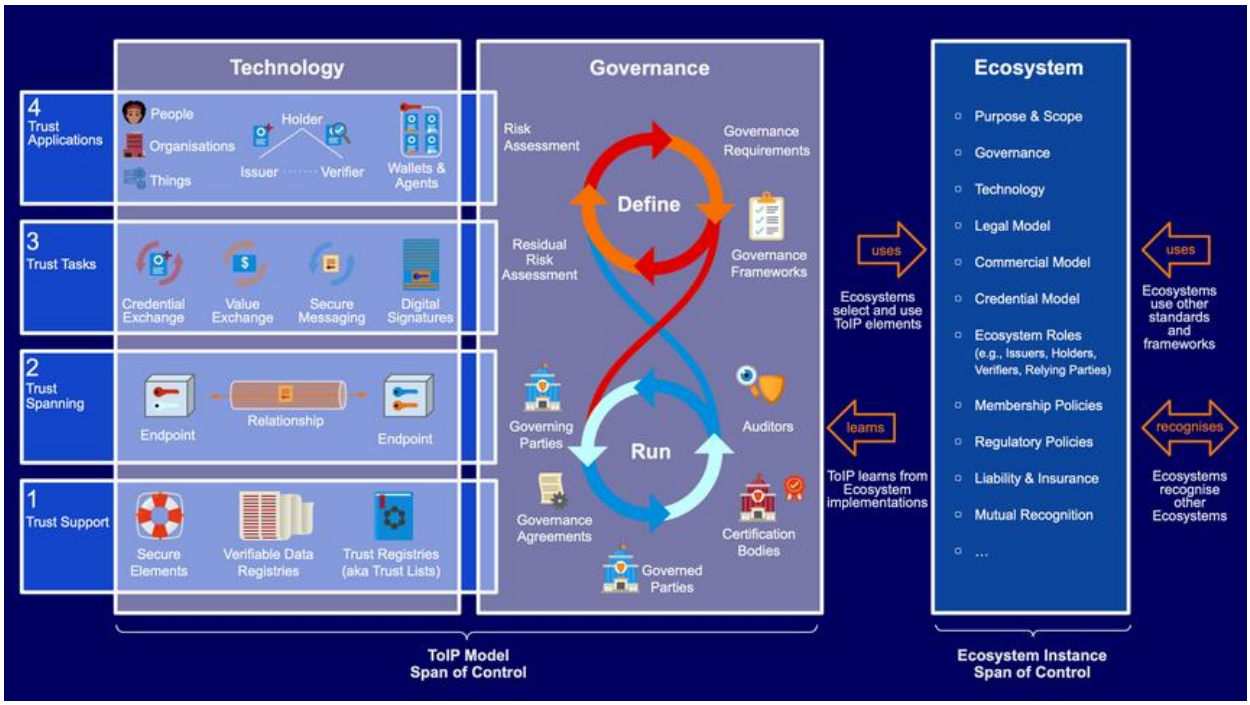

Figure 5: The Trust over IP Model (Source: Trust over IP Foundation)

With this approach, the governance framework starts with purpose and scope, and then focuses on a differentiated risk assessment to derive **a structured set of rules**, **policies, processes and standards** for implementation in the Interoperable Digital Twin Test Bed.

3.4. Language and Terminology

The following conventions SHALL be used in this document:

- The TF SHOULD be written in plain language.
- The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119

3.5. Purpose

The purpose of the 3DxVERSE ecosystem to enable diverse parties (organisations or people), and their related actors (human or machine delegates) to access and interact with interoperable digital twins for sustainable travel and living communities.

3.6. Scope (who and what the Trust Framework applies to)

Organisations, people and things (e.g. physical devices and their digital twins, algorithms) are within the scope of this trust framework which is a complement to Deliverable 4.1 (3DxVERSE Digital Commons Framework). To balance the *interests* and *incentives* of multiple stakeholders in the ecosystem and the unique impact that *decisions* based on simulations or visualisations that Digital Twin implementations can lead to, we consider that although this is fundamentally a digital governance framework, real-world impacts on the environment (e.g. air quality), the natural world (e.g. habitat loss, carbon emissions), and people (e.g. use of IoT devices for surveillance) are also in scope of this trust framework.

3.6.1. Roles in the 3DxVERSE ecosystem

The Trust Framework is designed to support the primary functions of entities (organisations, individuals or things) (including natural things) participating in the 3DxVERSE ecosystem. The following are the core roles that organisations can perform within the 3DxVERSE ecosystem, collectively Participants.

Governance Authority: In this case the 3DxVERSE Programme Board.

Providers: These are data service providers, algorithm or model providers, infrastructure providers, intermediary or support service providers, orchestrators and integrators.

Consumers: These are institutional / professional consumers, citizen / community users, intermediary or service consumers and innovators / entrepreneurs.

Observers: These include data stewards / ethics authorities, and observers such as regulators and other assurance (auditors, conformance assessment bodies and independent observatories).

See Annexe Detailed Roles & Responsibilities in 3DxVERSE.

These roles integrate fundamental EU concepts of Data Sovereignty, Open Data, Trustworthy AI and the role of data intermediaries. They align with those in the Common Carrier Layer, defined by the Centre of Excellence for Data Space Interoperability[4], those within the iSHARE Trust Framework, and those within the eIDAS 2.0 ecosystem.

3.6.2. Functions under the scope of the Trust Framework

There are functions at five life stages for 3DxVERSE participants.

Stage 0: Pre-boarding / Registration
Establishes the foundation for trust and eligibility by evaluating prospective participants, aligning them with legal and governance expectations, and preparing them for secure and compliant ecosystem entry.

Stage 1: Onboarding
Enables participants to formally join the ecosystem by assigning roles, registering governance actors, and defining policies and permissions in line with legal and ethical standards.

Stage 2: Provisioning
Activates secure interactions by enrolling entities, verifying identities, negotiating terms, and setting up the technical and legal conditions for trusted data and service exchanges.

Stage 3: Management
Maintains operational integrity and compliance by enabling monitoring, auditing, provenance tracking, and dynamic enforcement of rules and access rights.

Stage 4: Off-boarding
Ensures secure and accountable exit by managing data retention, resolving residual risks, and archiving governance records to preserve trust and compliance post-departure.

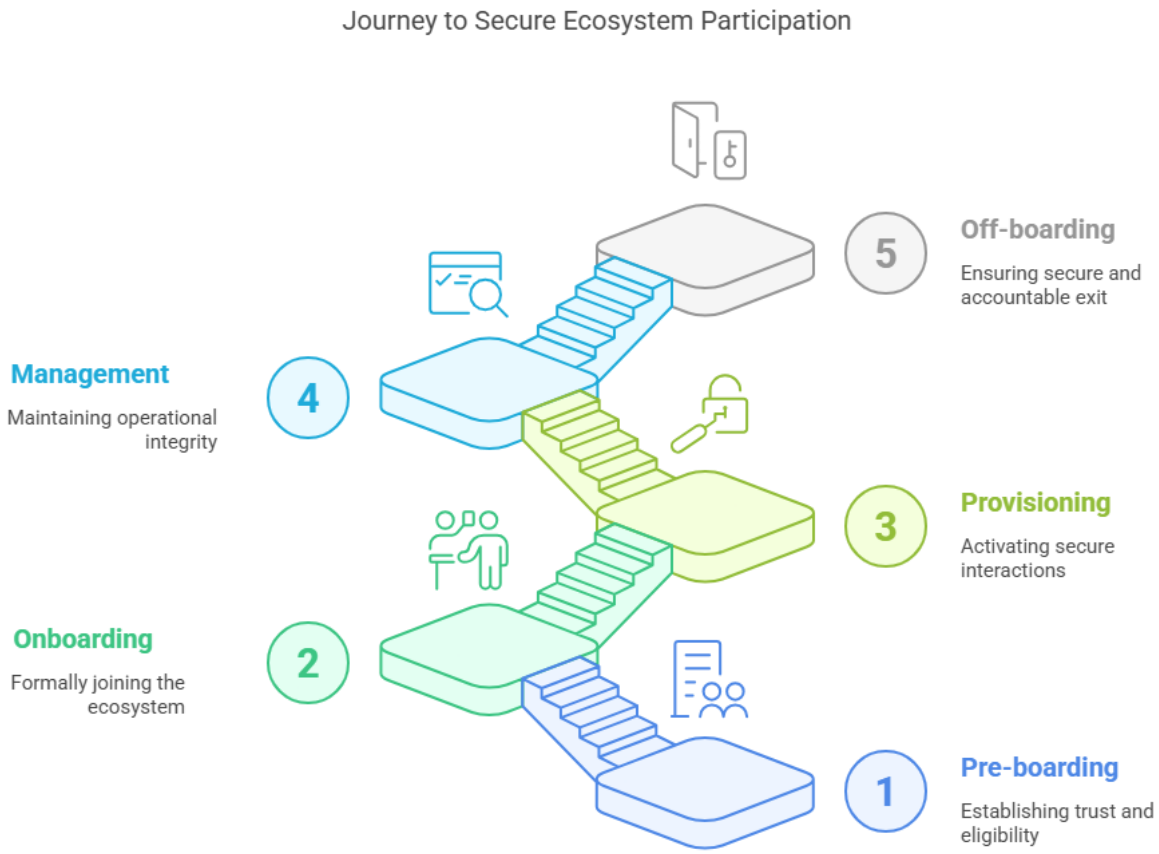

Figure 6: Overview of the scope of functions that the Trust Framework must support (image generated by Napkin.ai)

See Annexe for detailed functions as user stories and mapping to relevant EU legislation and standards.

3.7. Objectives (what the Trust Framework achieves)

- The security, privacy, safety, resilience, transparency, utility and interoperability of digital twin implementations and resources, e.g., the Local Digital Twin Toolbox within the 3DxVERSE ecosystem.
- Alignment with EU and Global Standards for digital twin implementations and resources.
- Support trustworthy relationships within and between digital twin ecosystems.

3.8. Principles (the values underpinning the Trust Framework)

The principles are defined in D4.1 Digital Commons Framework:

Principle	Description
Inclusion & participation	Everyone SHOULD have the opportunity to meaningfully engage in the design, use, and governance of digital commons. This principle emphasizes diverse representation, community involvement, and the active inclusion of underrepresented voices. Participation must be supported through transparency, trust, and opportunities for co-creation across all stages of a Digital Common's lifecycle.
Accessibility	Digital commons MUST be accessible to all, regardless of ability, language, literacy, or digital skill level. Accessibility ensures that barriers—technical, cognitive, social, or economic—are proactively addressed, enabling equitable participation and aligning with both ethical values and legal obligations.
Democratic Governance	Digital commons SHOULD be governed through democratic and participatory models, ensuring community members can co-create rules and decisions. Such governance fosters trust, accountability, and adaptability by reflecting shared values and enabling diverse voices to shape outcomes.
Data Privacy	Respect for data privacy is essential in the design and operation of digital commons. Individuals MUST retain control over their personal data, with transparent policies, strong safeguards, and compliance with legal standards that protect privacy rights and data sovereignty.
Sustainability	Digital commons SHOULD minimise environmental impact and promote responsible use of resources. Governance must account for the ecological footprint of digital infrastructure and explore ways to support green innovation and long-term environmental stewardship.
Fairness	All individuals SHOULD be treated equitably in access, participation, and outcomes. Including non-discrimination, fair data practices, balanced labour structures, and protection against algorithmic bias or exclusion in digital systems.
Transparency	Transparency builds trust by making decision-making, data use, and system operations open and understandable. Digital commons SHOULD clearly communicate governance processes, platform impacts, and technical details, including open access to source code where relevant.
Legal Compliance	Digital commons MUST comply with existing legal frameworks, including data protection, intellectual property, AI regulations, and cybersecurity laws. Legal compliance safeguards communities, ensures accountability, and protects the long-term viability of commons-based models.
Human Rights	Digital commons MUST uphold and protect fundamental human rights in the digital space. These include rights to privacy, freedom of expression, non-discrimination, and participation in digital life, as recognized in international and EU digital rights frameworks.

Open-Source	Open-source approaches promote collaboration, transparency, and shared ownership. By making code and knowledge freely accessible, digital commons SHALL foster innovation, enable collective improvement, and align with principles of openness and community governance.[5]

3.9. General Requirements (what the primary rules of the Trust Framework are)

We base our general requirements on the six facets of trustworthiness security, privacy, resiliency, robustness, ethics and reliability.

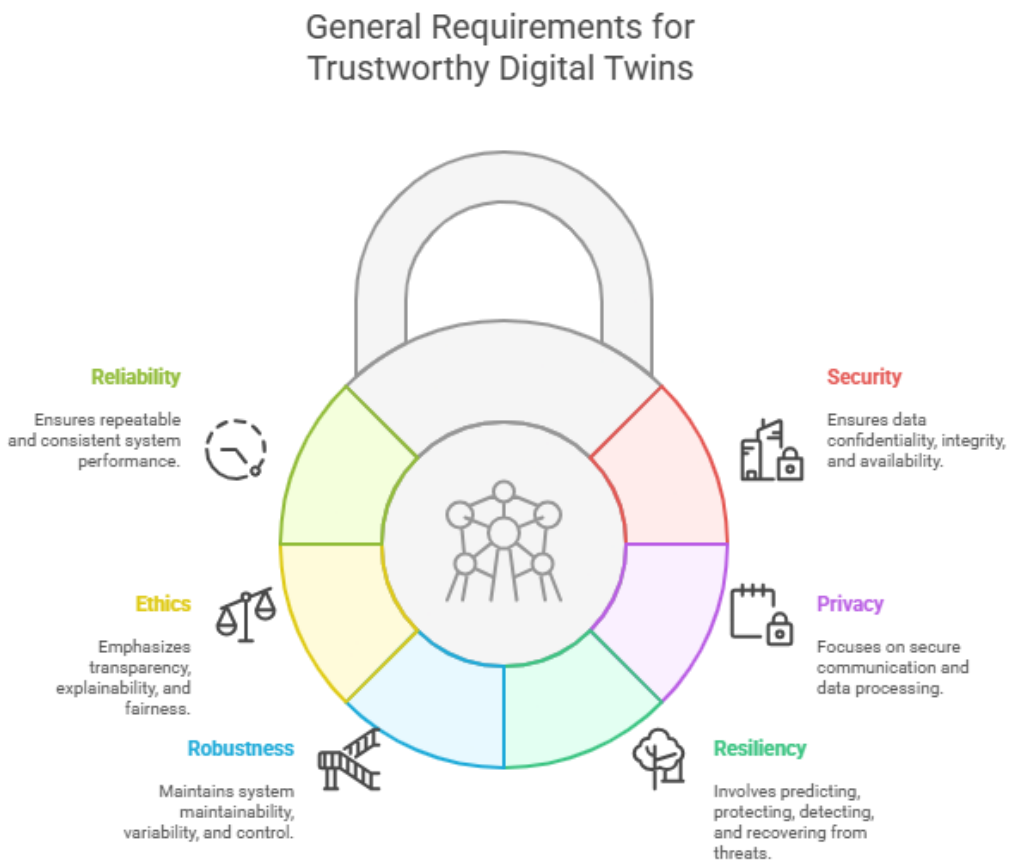

Figure 7: Illustration of the Facets of Trustworthiness. (Image generated by Napkin.ai; derived from Maple et al., 2021 Ref 2)

1. Security

- **Confidentiality**: MUST implement robust access control mechanisms to ensure that only authorized parties or systems can access data, algorithms or services.
- **Integrity**: MUST use cryptographic techniques to verify and maintain the accuracy and consistency of data during processing, storage, and transmission.
- **Availability**: MUST ensure system uptime through redundancy, disaster recovery planning, and responsive maintenance protocols.

2. Privacy

- **Communication**: MUST use end-to-end encryption to protect personal data during transmission and ensure it reaches only intended recipients.
- **Processing**: MUST limit data processing strictly to the purposes for which consent was obtained, and document consent management for transparency and accountability.

3. Robustness

- **Variability Control**: SHOULD design the system to handle unexpected inputs or changes in operating conditions without significant disruption to service.
- **Maintainability**: MUST ensure systems and components are designed for easy monitoring, diagnostics, and maintenance to restore serviceability efficiently.

4. Ethics

- **Transparency**: MUST maintain an audit trail of data, algorithm and service usage and decision-making processes that is accessible to users and auditors.
- **Fairness**: SHOULD ensure that system rules and processes are equitably applied to all users regardless of their background or status.
- **Explainability**: MUST provide users with understandable explanations for decisions or outcomes involving their identity data or access.

5. Reliability

- **Repeatable**: MUST ensure that lifecycle tasks (e.g., identity registration, software updates) can be executed consistently across users and sessions.
- **Consistent**: SHOULD implement systems to reconcile errors and maintain consistent data and behaviour throughout the DevSecOps lifecycle.

6. Resiliency

- **Predict:** SHOULD carry out penetration testing and use predictive techniques to maintain awareness of emergent threats.
- **Detect**: MUST include intrusion detection and system monitoring tools to identify incidents in real-time.
- **Protect**: MUST design layered safeguards (technical, operational, organizational) to ensure critical services remain available under threat conditions.
- **Recover**: MUST deploy and regularly test disaster recovery plans to ensure timely restoration of services after disruption.

3.10. Schedule of Controlled Documents

Controlled documents are part of the Trust Framework. As they are listed separately, they can be updated without requiring a complete re-issuance of the overall Trust Framework. All the controlled documents for this Trust Framework are in Annexes to this Report.

1. **Risk Management Process Summary and Risk Assessment aligned with the ENISA Risk Management Process.**

Identifies where we are in the ENISA (European Union Agency for Network and Information Security) Risk Management Process and includes The **Risk Assessment Logs** for the programme are attached in an embedded spreadsheet and cover:

- Project Risks, last updated 12 December 2024

- Stakeholder Risks against Trust Framework, last updated 16 April 2025
- Cybersecurity Risks, last updated 09 May 2025
- AI Risks, last updated 09 May 2025

2. **Security Policy**

Proposed security policy applicable to all participants

3. **Privacy Policy**

Proposed privacy policy applicable to all participants

4. **Information Security Policy**

Proposed information security policy applicable to all participants

5. **PLACEHOLDER Algorithmic Impact Assessment**

6. **PLACEHOLDER Data Protection Impact Assessment**

7. **PLACEHOLDER Human Rights Impact Assessment**

3.11. Change Control (how to revise the Trust Framework)

This Trust Framework and its associated policies and controlled documents are updated using the iterative process described in Adaptive and Machine Enforceable Governance in Chapter 5 below. This DRAFT document serves to provide INPUTS into the governance process alongside those deliverables from other Work Packages specifically 4.1 Digital Commons Framework, and 1.1 Ethics Requirements.

4. DRAFT DEVSECOPS FRAMEWORK

T2 *Draft* **DevSecOps Framework** describes how the policies, processes and compliance standards defined in the Trust Framework are implemented, maintained and assured in WP7 (Interoperable Digital Twin Testbed) and WP8 (Pilots and Citizen Engagement).

4.1. What is a Dev Sec Ops Framework?

DevSecOps integrates security into the software development lifecycle, ensuring that **development, security, and operations** are seamlessly combined. It aims to make security a shared responsibility across all teams involved in the software development process, ensuring that security is not an afterthought but is embedded throughout the entire IT lifecycle.

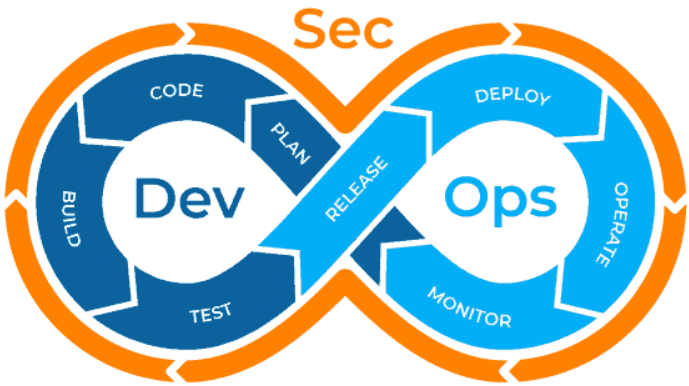

Figure 8: Illustration of DevSecOps Agile Process (Source: https://www.plutora.com/blog/devsecops-guide)

The Ideal goal is **"detect security issues (by design or application vulnerability) as fast as possible."** (Source OWASP[6])

4.2. DevSecOps Framework and Toolchain

3DxVERSE has begun to implement a State of the Art Secure Software Development and DevSecOps framework making use of the latest DevSecOps tools, standards, methodologies, tools and best practices. 3DxVERSE will be considering security across all phases of the Software Development Life Cycle (SDLC) and apply appropriate security measures on the corresponding assets that may be affected. The applicable frameworks, standards and tools (known as the toolchain) are described below.

A Reference Architecture Diagram will be made in Archimate to leverage the European Interoperability Framework (EIF) for DataSpaces, AI and Digital Twins and other Reference Architectures such as GAIA-X and other Digital Europe programs.

Miro will be used for collaborative analysis and modelling of the Digital Twin Ecosystem.

4.2.1. Plan & Define (Governance & Requirements)

- **Standards & Frameworks:**
  - OWASP Secure Coding Practices
  - Microsoft Secure Development Lifecycle Practices
  - ENISA Good Practices for Security of IoT - Secure Software Development Lifecycle
  - OWASP Software Assurance Maturity Model (for assessment)

- **Tools:**
  - **Confluence**: Requirements documentation and security design discussions.
  - **Atlassian Jira**: Security risk tickets, user stories, and backlog prioritization.

4.2.2. Code & Build (Development + Static Checks)

- **Secure Development Guidelines:**
  - Apple Secure Development Guidelines
  - Android Developer Security Documentation
  - OWASP Mobile Application Security

- **Tools**:
  - **IDE Plugins**: For secure coding (e.g., GitHub Copilot with security linting).
  - **GitHub**: Version control with branch protection rules and signed commits.
  - **GitLab**: Leveraging code.europa.eu for collaboration and advanced devsecops capabilities e.g. code assessments.
  - **Static Analysis (SAST)**: **SonarQube**, **Semgrep**, or **Checkmarx** for secure code analysis.

4.2.3. Test (Automated + Security Testing)

- **Security Testing Standards**:
  - OWASP Mobile Security Testing Guide

- **Tools:**
  - **OWASP ZAP / Burp Suite**: Dynamic App Security Testing (DAST)
  - **MobSF (Mobile Security Framework)**: Automated mobile app security testing
  - **Snyk** or **Dependabot**: Dependency scanning for vulnerabilities
  - **Postman** + **Newman**: API testing with security assertions
  - **Unit + Integration Testing**: Executed automatically via CI pipeline

4.2.4. Release (Containerization + Infrastructure Security)

- **Infrastructure Technologies:**
  - **Microsoft Azure Confidential Compute:** Certified high level of assurance hardware for containerization
  - **Docker / Nomad / Consul**: Containerization and service orchestration
  - **Kubernetes**: Orchestrating secure microservices
  - **PostgreSQL**: Secure database with encryption and audit logging

- Tools:
  - **Trivy / Clair / Anchore**: Container vulnerability scanning

- **Terraform / Helm**: Infrastructure as Code (IaC) with security policies

4.2.5. Deploy (CI/CD Integration + Secrets Management)

- **CI/CD Framework:**
  - **GitHub Actions / Azure DevOps Pipelines**: Automate testing, scanning, and deployment
  - **Vault by HashiCorp**: Secrets management and access control
  - **OPA (Open Policy Agent)**: Policy enforcement in Kubernetes deployments

4.2.6. Monitor & Respond (Runtime Security + Feedback Loop)

- **Tools:**
  - **Falco / Aqua Security**: Runtime container security and intrusion detection
  - **Azure Monitor / Prometheus + Grafana**: Observability and alerting
  - **ELK Stack / Loki**: Logging, anomaly detection, and pseudonymisation (ENISA recommendations)

4.2.7. Document & Improve (Knowledge Sharing + Maturity Assessment)

- **Tools:**
  - **Confluence**: Documentation of security decisions and post-mortems
  - **OWASP SAMM**: Maturity assessment across DevSecOps stages
  - **Archimate**: Reference architecture modelling (aligned with EIF, GAIA-X, Digital Europe)

4.3. Conformity Assessment and Certification

As part of the DevSecOps process 3DxVERSE will use conformance and certification pathways detailed in Annexe EU and Global Standards Alignment. The reference implementation of the Interoperable Digital Twins WP7 provided by ESRI on their ArcGIS platform complies with the following standards[7]:

Geospatial technology

ArcGIS supports reading and writing standard and common data file types using industry and international standard data formats, and via the web through OGC web services.

- Geospatial Formats: SHP, KML, GML
- Tabular Files: CSV, Excel, TDF, CDF
- Documents: JSON, GeoJSON
- Geospatial Standard Services: WFS, WMTS, WMS, WCS, WPS
- Metadata: ISO 19115, INSPIRE, DCAT, Dublin Core

Security and privacy

Security means exposing the right content to the right customers while protecting your enterprise. Esri complies with US government and international GIS standards as well as industry best practices for IT security and privacy.

- US Federal Government FISMA and FEDRAMP
- PCI Data Security Standard
- EU GDPR and the EU-US Privacy Shield Framework

- ISO 27001
- Open Web Application Security Project (OWASP) guidelines

Accessibility
Esri's goal is to design and implement accessible GIS and give people access regardless of their abilities.

- Alignment with W3C Web Content Accessibility Guidelines (WCAG) v2.0
- Alignment with Section 508 of the Rehabilitation Act of 1973 (US)
- Voluntary Product Accessibility Templates (VPAT) available for each ArcGIS product

IoT Security will be tested, assured and certified by Red Alert Labs for conformance with relevant standards, see Annexe EU & Global Standards alignment for current conformance, compliance and certification status of the WP7 Reference Implementation and Testbed provided by Esri together with the target compliance standards that we aim to achieve by the end of the programme.

4.4. Risk Management Framework

ENISA (European Union Agency for Network and Information Security) is an EU agency focused on cybersecurity, helping the EU and its member states predict, prevent, detect, and respond to information security problems. We will use their Interoperable EU Risk Management Toolbox (2023) which bases its approach on scenario's and use cases. The process is illustrated below with further detail provided in the Annexes.

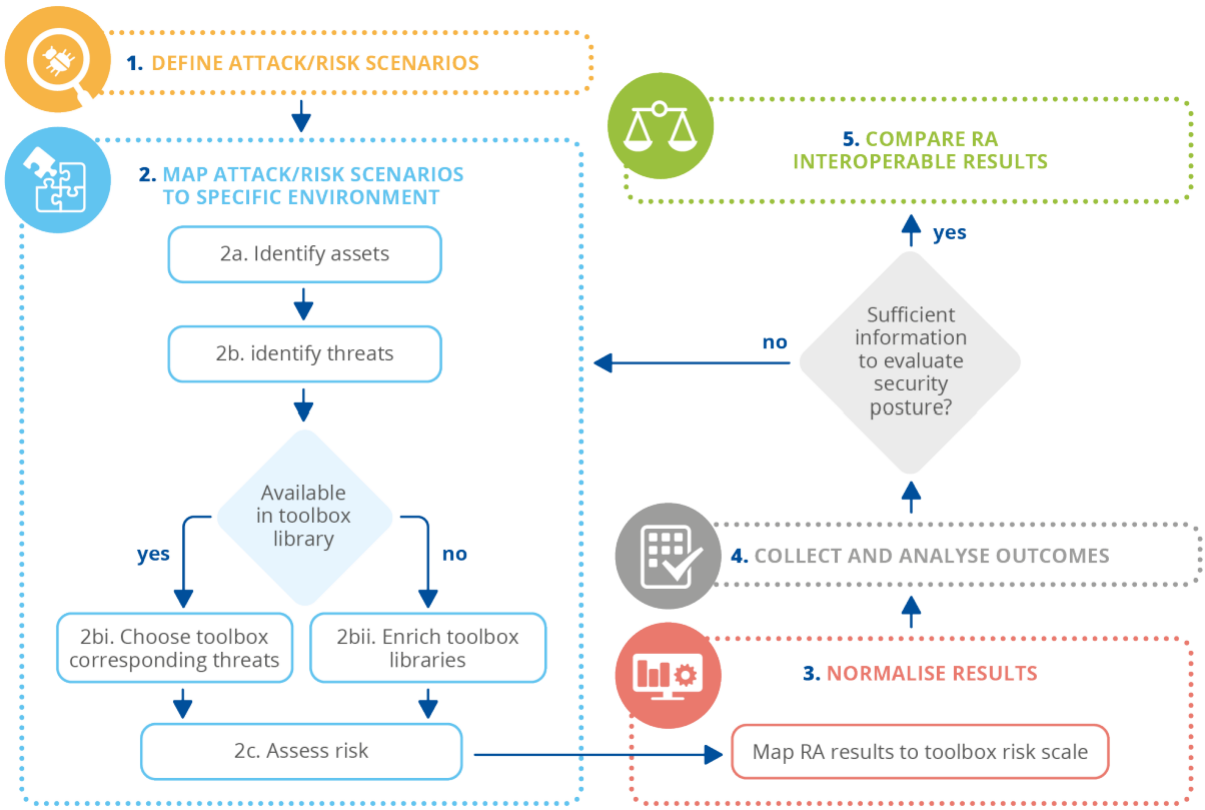

Figure 9: Interoperable EU Risk Management Toolbox Process (Source: ENISA)

4.4.1. Assets

The Primary Assets of 3DxVERSE include all the core business processes and functions as well as Services provided to external parties, and the Information and Data serving business processes and/or activities of the organisation. The Supporting Assets of 3DxVERSE include Hardware, devices and equipment, software and applications, roles, locations and utilities as well as the organisational infrastructure (e.g. policies, procedures and supporting ICT Services).

These will be documented using ENISA's Asset Mapping template.

4.4.2. Threat Landscape

Current Threats identified in the ENISA Threat Landscape 2024 (September 2024) will be prioritised for mitigation. These are classified as Wilful Attacks and will be documented using ENISA's Threats Mapping template.

- Ransomware
- Malware
- Social Engineering
- Threats against data
- Threats against availability (Denial of Service)
- Information Manipulation

Geopolitical threats also require planning for threats against unavailability or intrusion of critical data processing using the digital cloud infrastructure used by the partners. Many IT systems dealing with complex data processing, e.g., for estimating and verifying the carbon footprint of all user groups involved need access to private or public cloud infrastructure. With the so-called US Patriot Act, Cloud Act, and FISA 702 regulation U.S. authorities, such as CIA and FBI, have the right to request data without any suspicion of crime. What was a reaction to the 9/11 terrorist attack in 2001, is still an active regulation including all US cloud providers such as Microsoft Azure, Amazon AWS or Google and Apple. What might be acceptable for private use, becomes critical for business areas where EU and US are fully competitive, e.g. aviation industry (Airbus, Boeing, Earth Observation Satellites, etc.). To prevent dependencies from US cloud providers, the European Open Science Cloud Association (EOSC-A) was formed in 2020 under Belgian law giving guarantees that no personal data will be transferred to recipients outside EU.[8]

We consider that as the value of 3DxVERSE increases, so too does its **vulnerability.** The same report identifies prime 3DxVERSE sectors as vulnerable to attack with 63% of targets in reported events:

- Public Sector (33%)
- Transport (11%)
- Digital Infrastructure (8%)
- General Public (8%)
- Energy (3%)

We also take into account the ENISA Foresight Cybersecurity Threats for 2030 Update (March 2024) which identifies the following scenarios prioritising SCENARIO 2 and SCENARIO 4 as having particular relevance.

- SCENARIO 1 – BLOCKCHAIN, DEEPFAKES, & CYBERCRIME IN A DATA-RICH ENVIRONMENT
- **SCENARIO 2 – ECO-FRIENDLY, SUSTAINABLE, AND INTERCONNECTED SMART CITIES (NON-STATE ACTORS)**
- SCENARIO 3 – MORE DATA, LESS CONTROL
- **SCENARIO 4 – SUSTAINABLE ENERGY, AUTOMATED/SHORT-TERM WORKFORCE**
- SCENARIO 5 – LEGISLATION, BIAS, EXTINCTIONS, & GLOBAL THREATS

4.4.3. Risk Impact Levels

3DxVERSE will use the ENISA Risk Impact Definitions for likelihood and impact to manage and prioritise risk treatments.

4.4.4. Risk logging, review and treatment

As detailed in the process above, we will review risks at each stage in the agile development process. A risk log covering programme, cybersecurity, stakeholder and AI risks is available in Annexe Risk Management Process Summary and Risk Assessment.

4.5. Dual Use of Digital Twins: Enabling Resilience, Security & Strategic Readiness

3DxVERSE aims to operationalize dual-use digital twin capabilities, enabling both civilian and defence applications to leverage shared, trusted digital public infrastructure. As part of the EU's Critical Infrastructure strategy, digital twins will be deployed across public and military domains to ensure situational awareness, predictive resilience, and mission-critical decision support—while remaining fully compliant with European legal and cybersecurity frameworks.

Digital twins can support:

- Real-time network monitoring and cyber threat simulation in Security Operations Centres.
- Verification of configurations and policies in military-grade and civilian networks using digital replicas (network twins).
- Predictive maintenance and threat modelling for critical infrastructure like hospitals, energy grids, transportation hubs, and defence assets.
- Urban planning with military logistics foresight, e.g. planning routes and bridges for military convoys alongside civilian transport use.

To support this duality of purpose, 3DxVERSE will implement the following additional measures:

Governance & Legal Measures

- Role-based access control (RBAC) & attribute-based access control (ABAC) for segmented civilian/military use.
- Legal alignment with the EU Defence Procurement Directive 2009/81/EC
- Trusted Execution Environments (TEE) and secure onboarding for military actors under eIDAS 2.0

Security & Compliance Measures

- Compliance with NIST 800-207 (Zero Trust Architecture)
- Integration with NATO Federated Mission Networking (FMN) standards for interoperable defence systems.
- Layered defence using secure-by-design DevSecOps, code signing, intrusion detection, and multi-cloud resilience.

3DxVERSE will work with WP8 to evaluate **Operational Readiness Use Cases**, for example;

- Joint emergency simulations for climate disaster response and cyber incidents.
- Digital war-gaming and training environments for military and civil protection agencies.
- Support for UAV/drones and autonomous surveillance systems under EU defence innovation.
- Secure digital twin sandboxes for classified defence transport and energy scenario modelling.

In aligning defence innovation with civil resilience, 3DxVERSE ensures that digital twin technology remains a force multiplier for security, sustainability, and sovereignty—empowering EU states and allied partners to adapt to complex threats and opportunities alike.

4.6. Analysis of Trust Lists and Trust Registries

Trust Lists and Trust Registries are mechanisms used to establish, publish, and manage trusted relationships in digital systems. They are essential for verifying identities, credentials, and communications in secure and interoperable environments.

A **Trust List** is a static or semi-static list of trusted entities, typically including certificate authorities (CAs), public keys, or trust service providers. Trust lists are used in:

- TLS/SSL (e.g., browser root stores)
- Digital signatures (e.g., Adobe AATL, EU Trusted Lists)
- Document and email validation
- eIDAS-compliant services in the EU

They are often centrally managed by a standards body or vendor, and trust decisions are made based on pre-approved inclusion.

A **Trust Registry** is a more dynamic, database or ledger that can be queried by the Trust Registry Query Protocol[9], it records who is trusted, for what, and under what conditions. Trust registries are used in:

- Verifiable credentials and digital identity ecosystems
- Decentralized ID systems (DIDs)
- OpenID federations
- Blockchain-based governance models

Trust Registries allow for decentralized trust, support real-time updates, and often offer APIs to register, discover, and verify trust anchors, schemas, or credentials.

In practice Trust Lists are used by browsers to validate websites. Whereas digital wallets, agents or applications use Trust Registries to verify credential issuers or verifiers (as an anti-coercion measure) and to validate verifiable credentials. Federated identity systems rely on Trust Registries to dynamically discover trusted identity providers.

Together, they form the backbone of secure, interoperable digital trust systems that rely on trust authorities and cryptographic trust roots to verify, authenticate, and authorise transactions or to validate data authenticity and provenance.

See Annexe Trust Lists & Trust Registries for a comparative overview of global Trust Lists and Registries, detailing their scope, managing entities, API availability, and common use cases such as digital identity, credentials, and cybersecurity. It includes centralized systems like EU Trusted Lists and Adobe AATL, as well as decentralized and federated models like OpenID Federation, and blockchain-based registries.

5. PRIVACY, SECURITY AND VALUE CREATION BY DESIGN

This chapter explains how we will support engagement with citizens in WP4 (Digital Commons), (WP6 Use Case Design) and WP 8 (Citizen Engagement & Pilots), as well as delivering new content for the Local Digital Twin Toolbox, the European Interoperability Toolbox and the New European Bauhaus Toolbox. The chapter first outlines the project iterations which apply to each use case across three workstreams: Social Design, Governance (Trust Framework) and Technology. We then explain the Agile Development process and Backlog prioritisation approach that we will use based on product KPI's (Key Performance Indicators). Finally, the chapter includes some practical recommendations for ecosystem participants in WP's 4, 6 and 8.

5.1. Socio-Technical Systems Design in Practice

A **socio-technical system** is a system that involves a complex interaction between people (social elements) and technology (technical elements) within an environment. It emphasizes that effective design, implementation, and use of technology must consider both human and technical factors together—not in isolation.

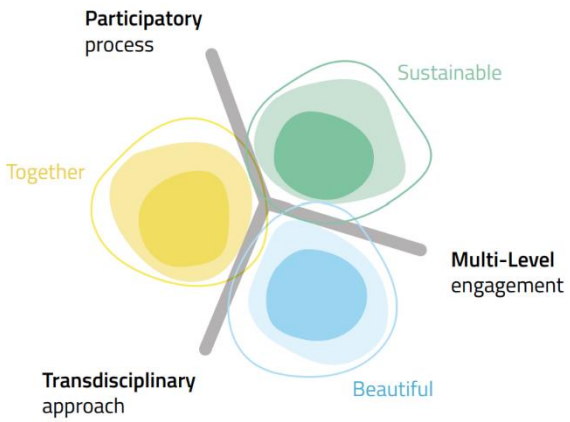

Figure 10: The New European Bauhaus Compass - Participatory Process, Transdisciplinary approach and Multi-Level Engagement (Source: NEB Toolbox, Ref 10)

3DxVERSE is citizen-centric socio-technical system and will base its design and development practice on the New European Bauhaus (NEB) Compass, *a guiding framework for decision and project-makers wishing to apply the NEB principles and criteria to their activities*.[10] We will adapt the NEB Toolbox[11] which defines best practices for citizen co-design throughout three phases of a real-world architectural or planning project: Identification, Exploration and Refinement. We adapt these to align with participatory and socialised design processes based on inclusive design and social research methods used in commercial product development.

The diagram below illustrates how 3DxVERSE engages citizens during identification, exploration, and refinement phases, aligning with adaptive governance and the Trust Framework, and integrating with the DevSecOps delivery process.

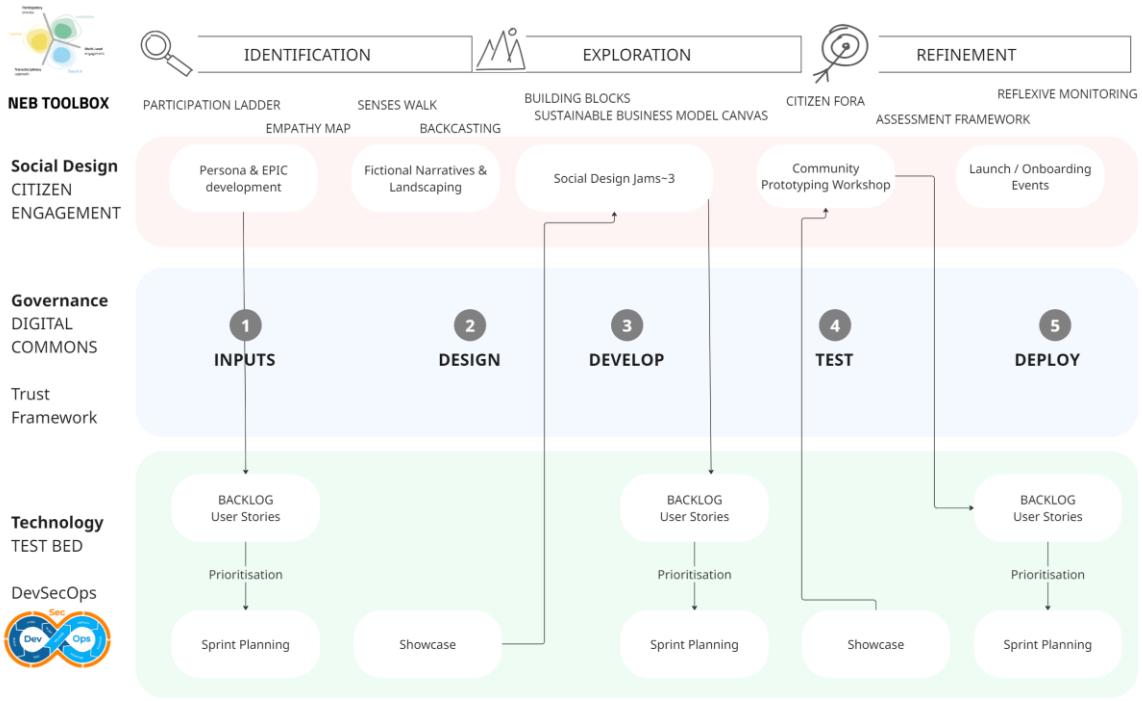

Figure 11: Illustration of the per use case iteration showing social design, governance and technology

5.2. Proposed Timeline of Iterations for Use Cases

Using iterations as described above, we will plan the programme delivery in five releases:

1: Core Lifecycle and Use Case Integrations
2: Pilot Preparation to support WP6, WP7 and WP8 deliverables
3: Pilot Start-Up including pre-boarding and on-boarding for pilot participants
4: As Required New Use Cases and Integrations which may for example include new data spaces, new local digital twins, new technological capabilities, new regulation or standards or new requirements from new user groups.
5: The final iteration will focus on packaging for delivery to NEB, Local Digital Twin and Interoperable Europe Toolboxes.

The high level proposed plan addresses the following use cases:

UC 0 3DxVERSE Core These are core generic capabilities or functions that apply to all application use cases. This document specifies the Roles and Lifecycle User Stories (See Annexes) that must be satisfied in the first iteration in preparation for supporting subsequent application use cases (UC1, 2 and 3). It will be followed by Iterations for Feature Enhancements and Packaging for inclusion in delivery use cases (UC4,5 and 6).

UC 1 Sustainable Living Communities, UC 2 Sustainable Airport and Living Environment, UC 3 Sustainable Mobility. These are application use cases which tailor the Core with capabilities or functions which may require education, configuration or development and are primary deliverables for WP6 (Use Case Design) and WP 8 (Citizen Engagement and Pilots). It is expected that we will have two iterations for each use case, but the second iteration may be shorter. We will adapt and utilise capacity as required to maintain a performant capability.

UC 4 NEB Toolbox, UC 5 Local Digital Twin Toolbox and UC 6 Interoperable Europe Toolbox are all delivery use cases which will package the tools (including documentation) for inclusion in the relevant toolboxes for reuse by other EU projects.

UC 7 Cybersecurity & Compliance Updates these are not socially designed but will essentially act as a trust assurance use case that evaluates the privacy and security of 3DxVERSE and conformance against compliance requirements specified in Annexe EU & Global Standards Alignment. The final update will be D5.2 Cybersecurity and Compliance Report.

Phases 'Releases'	R1: Core Lifecycle & Use Case Integrations				R2: Pilot Preparation			R3: Pilot Start-Up			R4: As Required New Use Cases and Integrations									R5: Packaging for NEB, LDT & Interoperable Europe Toolboxes					
	May	Jun	Jul	Aug'25	Sep	Oct	Nov	Dec	Jan	Feb'26	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov '26	Dec	Jan	Feb	Mar	Apr	May '27
	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24	M25	M26	M27	M28	M29	M30
UC0 3DxVERSE Core	ITERATION - Lifecycle										ITERATION - Feature Enhancements											ITERATION - Packaging			
UC 1 Sustainable Living Communities					ITERATION								ITERATION												
UC 2 Sustainable Airport & Living Environment						ITERATION								ITERATION											
UC 3 Sustainable Mobility							ITERATION								ITERATION										
UC 4 NEB Toolbox																		ITERATION							
UC 5 Local Digital Twin Toolbox																			ITERATION						
UC 6 Interoperable Europe Toolbox																				ITERATION					
UC7 Cybersecurity & Compliance Updates					1									2											3

Figure 12: Snapshot of the high-level implementation plan showing use case iterations against a timeline of releases

5.3. Adaptive, Machine Enforceable Governance

The Digital Twin and AI Trust Framework detailed above is also an agile process that links with DevSecOps. The diagram below illustrates how a governance (or Trust) framework is iteratively created and linked with the technical and business architecture. This method, using domain modelling to develop governance frameworks, has been proven to effectively support participatory design processes through visualisation and clear definition of different ecosystem layers and to promote the development of more systemic and robust governance.[12]

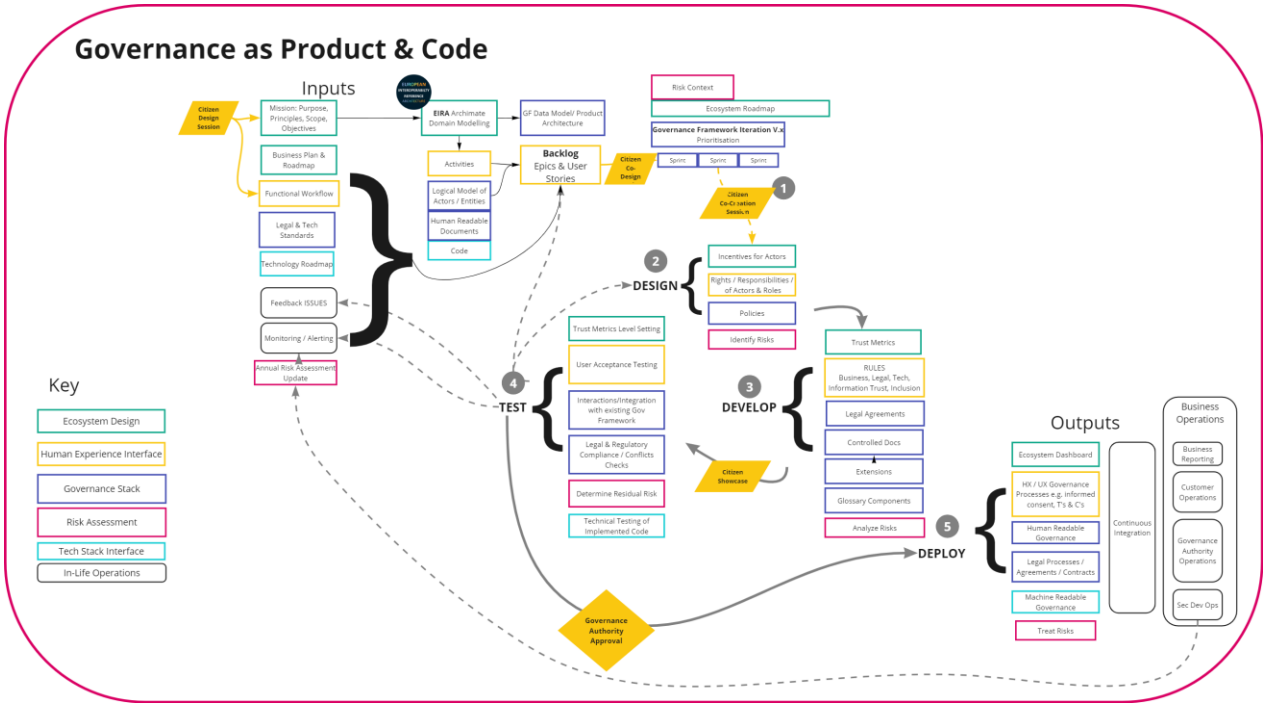

Figure 13: Illustration of the process by which Trust Framework is developed and operated for adaptive, machine enforceable governance

3DxVERSE will leverage the European Interoperability framework (EIF) and European Interoperability Reference Architecture (EIRA[13]) to ensure creating interoperable digital twin solutions by design based on the same architecture tools (the Archi Tool and ArchiMate® language and the Interoperability Testbed (ITB)). This is mandatory by the Interoperable Europe Act for all the digital public services in European Union.

This document together with the inputs from D4.1 Digital Commons Framework, D1.1 Ethics Framework and the requirements specified in D3.1 Reference Architecture form the basis for Inputs (1) in this model above.

5.4. Technology: Agile Development and Backlog

We have implemented the PM2 Project Management Methodology 3.1 Agile Extension with daily Standups, layered iterations and five major releases.

Now that the SOTA Interoperable Digital Twin Test Bed is available, we will create a backlog of user stories that cover the 3DxVERSE Core lifecycle requirements common to all application use cases. These are documented in Annexe: Detailed Functions as User Stories aligned against EU Standards and Regulation.

Governance, business and user requirements from WP4 Digital Commons; the Digital Twin and AI Trust Framework (this document), WP 6 Use Case Design and WP 8 Pilots and Citizen Engagement. Other generally more technical requirements arise from WP 3 (Reference Architecture), WP 7 (Testbed) and may also arise from security monitoring, new interconnections, new software updates, new compliance requirements and new technologies implemented in line with the roadmap described in D3.1.

These requirements are documented as user stories or epics using Jira and triaged as either ***education*** (training, guidance or assistance required)**,** ***configuration*** (requires system configuration), ***or development*** (requires new code).

5.5. Product KPI's as Prioritisation Criteria

Prioritisation criteria are to be confirmed with stakeholders but from a product capability they will be against the following KPI's that are the basis for measuring not only trustworthiness, but also performance and value creation. All tickets in the backlog will be scored against the extent to which they agree to:

It is secure and private: *Incidents, Pen-test success.* Measured through incident log #'s reported, resolved, outstanding including level of risk. Measured through penetration testing and reports on security monitoring and controls and compliance evaluations.

It works: *Availability & Response Times.* Measured end-to-end including in constrained environments (e.g. limited power, limited connectivity)

It scales: *Participant, Geospatial, Simultaneous Users.* Measured based on stress and dimension testing to be carried out at the same time as each major release, represents the total capacity.

It creates value: Measured against *dimensions of data market growth*:

Reach: Number of users (individual citizens or organizations), number of devices, percentage global geospatial reach (3 dimensions).

Density: Number of data, algorithm and service providers consumed per user.

Frequency: Average number of transactions / interactions per week per user.

It is participatory: % participants (providers, consumers, observers) that are *actively engaged in governance* via the digital commons process defined in D4.1.

The prioritised user stories will then be planned in development iterations and major releases as appropriate. Each release should increase performance against KPI's above. We will baseline the KPI's and set targets with other teams in the project by end June 2025. This Trust Metrics setting is part of the adaptive, machine enforceable governance process.

5.6. Practical recommendations for ecosystem participants in WP6 (Use Cases) and WP8 (Pilots and Citizen Engagement)

Standards, principles, even policies will only go so far. This part of the document outlines practical guidance for trustworthy service design in line with the principles outlined in the Trust Framework and the 3DxVERSE citizen-centric vision.

Use of persona and storytelling:

Participatory and co-creative design processes are complex, time-consuming and often costly. It is difficult to meet the objectives of inclusive and respectful design processes at the same time as keeping up with the demands of technology, innovation and business for speed and return on investment. At the same time, it can be difficult to articulate complex technologies or concepts to truly diverse groups of citizens. We recommend the use of design thinking and use of persona including edge-case / extreme

user persona to develop clearly constructed user stories that are inclusive by design, and the use of bad actor persona to ensure that a system is designed *not* to meet their needs.

iLabs will offer a 3 hour persona and storytelling work-based learning workshop to 3DxVERSE community leaders and team members to support common understanding and techniques, developing a library of persona with their user stories that enable diverse, secure and inclusive development of the 3DxVERSE. We will also explore a technique of training an AI agent to act as a persona for user testing.

Own the outcome:

Citizens, organisations and communities should own the outcome. This practically means that they define and set the metrics for 3DxVERSE and sub-metrics for their use cases, and are thus able to prioritize the work of the 3DxVERSE team. Set metrics for your use case that relevant stakeholders will recognise as delivering value for them.

iLabs will coordinate the Trust Metrics process as part of Adaptive, Machine Enforceable Governance.

Practice Harms Reduction:

Nothing can ever be 100% de-risked and we are all exposed to harms in the digital world just as we are in the physical one. There are several techniques for harms reduction which are detailed in the Practical Steps for Overcoming Human Harm Challenges in Digital Identity Ecosystems from Trust over IP Foundation. We will evaluate together with those who have participant touchpoints (WP4, 6, 8) which of these measures are most relevant to their work.

Always ask 'What could possibly go wrong?'

When developing user stories against your persona, make good use of bad actor persona who are *not* to be satisfied. Develop user stories for failure scenarios and consider both direct harms (e.g. identity theft, fraud), indirect harms (e.g. bias, misinformation), contingent harms (e.g. impacts of opening a floodgate, trade-offs for commercial vs environmental sustainability), and felt harms (e.g. mental or physical health impacts). [14] Document these in our Risk Log.

iLabs can offer a 1 hour workshop on harms reduction and techniques for applying the Trust over IP Harms Framework.

Using the stakeholder risks in the risk log as a basis we will integrate differential risk management into the DevSecOps process.

6. CONCLUSIONS – 3DxVERSE AT THE FRONTIER OF TRUSTWORTHY DIGITAL TWINS

The **3DxVERSE project** establishes a new benchmark for the governance, development, and adoption of large-scale **Digital Twin ecosystems** that are secure, interoperable, and citizen-centric. This document outlines a set of foundational innovations introduced by 3DxVERSE, positioning the initiative as a European flagship for responsible digital transformation.

3DxVERSE sets a new benchmark for how large-scale digital-twin programmes can be governed, built and adopted with confidence. This document highlights key 3DxVERSE innovations as follows:

1.Machine-enforceable, full lifecycle governance: the **Digital Twin & AI Trust Framework** transforms high-level ethical and regulatory principles into **automated, enforceable policies**. It maps governance across a five-stage lifecycle—covering individuals, organisations, and devices—through rules directly interpretable by **DevSecOps pipelines**. Integrated **risk logs**, **change management mechanisms**, and **ENISA-aligned metrics** ensure that trust is not merely audited periodically, but maintained **continuously and adaptively**.

2.A DevSecOps tool-chain tailored to interoperable twins: security is embedded throughout the software development lifecycle—from **code commit to runtime**—using a tailored DevSecOps stack that incorporates **OWASP best practices**, **cloud-native vulnerability scanning**, **confidential computing**, and **Kubernetes policy enforcement**. The toolchain is directly aligned with **EU conformity frameworks**, **Gaia-X**, and **European Interoperability Framework (EIF)** reference architectures.

3.Hybrid trust authority model: 3DxVERSE introduces a **hybrid trust model** that bridges traditional trust infrastructures (e.g., **eIDAS LOTL**, **Adobe AATL**, browser root stores) with **dynamic trust registries** supporting **verifiable credentials (VCs)** and **decentralised identifiers (DIDs)**. This unified approach enables **seamless, cryptographic trust** across centralised and decentralised ecosystems, enhancing both compliance and innovation capacity.

4.Secure dual-use enablement for civil and defence needs: a **segmented access-control architecture** and layered compliance mechanisms allow the same digital twin infrastructure to meet the needs of **civilian smart-city applications** and **mission-critical defence scenarios**. The model complies with **NATO FMN**, **NIST 800-207 Zero Trust Architecture**, and **EU defence procurement regulations**, ensuring robust support for **dual-use applications**.

5.Socio-technical design anchored in the New European Bauhaus: 3DxVERSE integrates **participatory design methods** from the **New European Bauhaus (NEB)** into agile development processes, ensuring that each release prioritises **inclusion**, **aesthetics**, and **sustainability**. Techniques such as **AI-generated personas** and **co-creation workshops** help identify and mitigate **edge-case harms**, embedding **human values** into the system architecture from inception.

6.Value-centric KPIs and continuous risk telemetry: beyond traditional technical metrics (e.g., uptime, latency), 3DxVERSE introduces **value-driven KPIs** such as **stakeholder reach**, **trust event frequency**, **participation rates**, and **risk telemetry**. These metrics are embedded into the **governance fabric** and mapped to **ENISA risk frameworks**, enabling real-time adaptation to evolving operational and ethical conditions.

7.Standards-aligned interoperability testbed and identity connector: through a collaboration with **ESRI**, **iLabs**, and the **European Commission's Interoperability Test Bed**, 3DxVERSE offers an **extensible testbed environment** for conformance testing, certification, and onboarding. It supports a full spectrum of **cross-sector interoperability** and **decentralised identity integration**, enabling adoption at both **EU** and **global scales**.

Collectively, these innovations transform Digital Twin deployments from **isolated pilots** into a **cohesive, scalable, and citizen-first digital public infrastructure**. By combining **automated compliance**, **participatory governance**, and **cross-domain security**, 3DxVERSE not only meets the regulatory demands of today but also anticipates future challenges linked to **AI governance**, **digital sovereignty**, and **climate-aligned digital development**.

The 3DxVERSE project thus serves as a **template for future European and international initiatives** seeking to leverage Digital Twins in support of **sustainable**, **secure**, and **trustworthy growth**.

7. ANNEXES

7.1. EU Legislative Requirements

The following is a list of the relevant EU Legislation and Regulations that underpin the Trust Framework and which should be implemented in the 3DxVERSE project.

- **Cybersecurity Regulation,** (January 2024), aims to establish a high common level of cybersecurity at EU institutions, bodies, offices, and agencies. It mandates the creation of an internal cybersecurity risk management framework tailored to each entity's needs.

- **Cyber Resilience Act**, (December 2024), establishes common cybersecurity standards for products with digital elements, such as hardware and software. These products must meet specific cybersecurity requirements throughout their lifecycle, including automatic security updates and incident reporting.

- **Cyber Solidarity Act,** (February 2025), aims to improve preparedness, detection, and response to cybersecurity incidents across the EU.

- **Artificial Intelligence (AI) Act,** (from August 2026), establishes a risk-based framework to ensure AI systems are safe, transparent, and respect fundamental rights.

- **European Digital Identity Framework** – Regulation (EU) 2024/1183, (May 2024), mandates that EU Member States provide at least one European Digital Identity Wallet to citizens and residents by 2026, enhancing secure and seamless digital identification across the EU.

- **Digital Services Act (DSA) – Regulation (EU) 2022/2065**, (February 2024), sets out new obligations for online platforms to tackle illegal content, ensure transparency, and protect users' rights, aiming to create a safer digital space.

- **Data Governance Act (DGA) - Regulation (EU) 2022/868,** (May 2022), aims to regulate the reuse of publicly/held, protected data, by boosting data sharing through the regulation of novel data intermediaries and by encouraging the sharing of data for altruistic purposes.

- **Interoperable Europe Act – Regulation (EU) 2024/903**, (March 2024), aims to enhance cross-border interoperability and cooperation in the public sector across the EU, facilitating seamless digital public services.

- **Data Act – Regulation (EU) 2023/2854,** (from September 2025), establishes rules on fair access to and use of data, promoting a competitive data market and ensuring data is more accessible for businesses and public sector bodies.

- **NIS2 Directive – Directive (EU) 2022/2555,** (October 2024), strengthens cybersecurity requirements across the EU, expanding the scope to more sectors and introducing stricter supervisory measures and enforcement requirements.

- **General Data Protection Regulation (GDPR)** – Regulation (EU) 2016/679, (May 2018), sets the standard for data protection and privacy in the EU, granting individuals greater control over their personal data and imposing strict obligations on organizations processing such data.

7.2. Disaster Recovery & Business Continuity Plan

7.2.1. Introduction

Given the critical nature of this project, it is essential to have a robust Disaster Recovery and Business Continuity Plan (DRBCP) to ensure the project's resilience and continuity in the face of potential disruptions. The 3DxVERSE project is committed to ensuring the resilience and continuity of its operations through a comprehensive DRBCP. By implementing the strategies outlined in this plan, the project aims to minimize the impact of disruptions and ensure the quick recovery and continuity of critical functions.

7.2.2. Objectives

The primary objectives of this DRBCP are:

- To ensure the safety and security of all stakeholders involved in the 3DxVERSE project.
- To minimize the impact of disruptions on the project's operations.
- To ensure the quick recovery and continuity of critical project functions.
- To maintain compliance with relevant regulations and standards.

7.2.3. Risk Assessment

Potential risks to the 3DxVERSE project are documented in the Annexe Risk Management Process Summary and Risk Assessment.

7.2.4. Disaster Recovery Strategy

7.2.4.1. Data Backup and Recovery

- Implement regular data backups for all critical project data, including Digital Twin models, AI algorithms, and user data.
- Store backups in multiple secure locations, including off-site and cloud storage.
- Test data recovery procedures periodically to ensure they are effective and efficient.

7.2.4.2. Cybersecurity Measures

- Implement robust cybersecurity measures, including firewalls, encryption, and intrusion detection systems.
- Conduct regular security audits and vulnerability assessments.
- Train all project personnel on cybersecurity best practices and protocols.

7.2.4.3. Redundancy and Failover

- Establish redundant systems and failover mechanisms for critical project infrastructure, including servers, networks, and power supplies.
- Ensure that all critical systems have backup power sources, such as uninterruptible power supplies (UPS) and generators.

7.2.5. Business Continuity Strategy

7.2.5.1. Communication Plan

- Develop a communication plan to ensure timely and accurate information dissemination during a disruption.
- Establish communication channels with all stakeholders, including project personnel, partners, and regulatory authorities.
- Designate a crisis management team responsible for coordinating communication efforts.

7.2.5.2. Continuity of Operations

- Identify critical project functions and prioritize their recovery.
- Develop and document procedures for maintaining essential operations during a disruption.
- Establish remote work capabilities for project personnel to ensure continuity of operations.

7.2.5.3. Collaboration with Partners

- Collaborate with key partners, such as the International Data Spaces Association and Open & Agile Smart Cities (OASC), to ensure interoperability and support during disruptions.
- Establish mutual aid agreements with partners to provide assistance and resources during emergencies.

7.2.5.4. Testing and Maintenance

- Conduct regular drills and simulations to test the effectiveness of the DRBCP.
- Review and update the DRBCP periodically to reflect changes in the project, technology, and regulatory environment.
- Ensure that all project personnel are familiar with the DRBCP and their roles and responsibilities during a disruption.

7.3. Interoperability Testbed (ITB) for Interoperability Testing and Validation

3DxVERSE will be leveraging the Interoperability Test Bed as this has been also selected by OASC (Open and Agile Smart Cities) MIMs (Minimum Interoperability Mechanisms) Plus interoperability conformity assessments and also by the SIMPL project for federation of data spaces and has been used by iLabs for their EUDI Wallet Interoperability Testing to support latest FIDES Plugfest for Interop Testing of OpenID4VC. Its **open-source** nature makes it an ideal choice to provide transparency and to foster collaboration between the different parties involved in the testing process. From a technical perspective, its **extensible architecture** figures as a particular strong point, as it allows the use of custom extensions and integration of existing solutions to cover the various MIMs Plus requirements being tested. Finally, its **user friendliness** ensures easy and intuitive use even by those with limited technical experience.

To realise the conformance test scenarios, the MIMs Plus test plans are first expressed as GITB TDL test cases that can be processed by the Testbed. Upon execution, these test cases leverage the Testbed's built-in capabilities, with the addition of an internal JSON validator to cover data validation needs. Besides recording test results, the Testbed then also provides detailed test reports and technical logs to allow troubleshooting in case of failures.

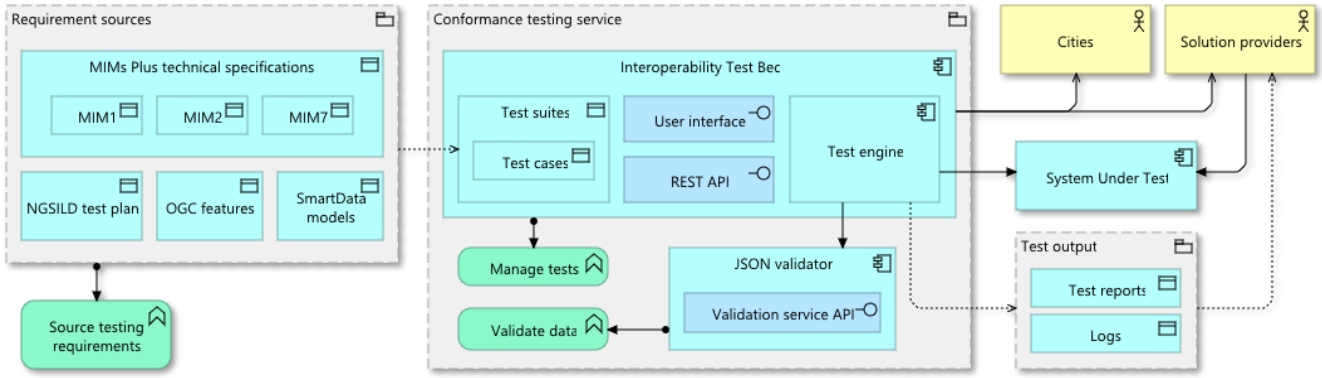

Figure 14: OASC MIMs Plus Conformance Testing

The conformance testing solution is expected to be made available to communities and solution providers by **mid-2025**. This first release will cover the more mature MIMs Plus, notably the MIM Plus 1 (Context Information Management), MIM Plus 2 (Data Models), and MIM Plus 7 (Spaces).

The goal is to progressively achieve **full conformance test coverage** as the maturity of the MIM Plus framework evolves. This testing work will also be integrated into a MIM Plus **certification scheme**, which is currently being developed by the consortium in ITU Y.4505 format

The goal of this certification initiative is to provide an even higher level of confidence for cities, communities, and regions when procuring interoperable solutions.

Before its official launch you will be able to explore the new testing platform at the upcoming Smart City Expo, which will be held between the **5th and 7th of November in Barcelona**, at the European Commission's booth. Current planning foresees also a live demo of the platform, allowing you to already test a system for conformity to MIMs Plus.

7.4. EU & Global Standards alignment

This Annexe details both EU and global standards that are required for alignment and compliance with the legislation and regulation. Certification or conformance as of May 2025 are highlighted in green. Throughout the lifetime of the programme we will implement conformance, this will be reported as part of our Cybersecurity and Compliance Updates and detailed in D5.2

7.4.1. Privacy Standards

This table lists the primary privacy and data protection standards in operation together with certification or conformance requirements where relevant. Certification or conformance as of May 2025 are highlighted in green.

Table 1: Privacy Standards Alignment

Name	Description	Scope	Certification / Conformance	Link to Certification
General Data Protection Regulation (GDPR) & EU/ US Privacy Shield	EU regulation on personal data protection.	EU	No official EU certification; ISO/IEC 27701 can support compliance.	https://www.iso.org/standard/71670.html
Data Governance Act (DGA)	Trust-based data sharing regulation.	EU	Compliance demonstrated via trusted data intermediaries and frameworks.	https://digital-strategy.ec.europa.eu/en/policies/data-governance-act
ePrivacy Regulation (Draft)	Regulation on electronic communications and metadata.	EU	Not in force; conformance mechanisms pending.	https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation
ISO/IEC 27701	Privacy Information Management System standard.	Global	Certification via ISO/IEC 27006-accredited bodies.	https://www.iso.org/standard/71670.html
ISO/IEC 29100	Privacy framework with principles and vocabulary.	Global	Not certifiable; used for policy design.	https://www.iso.org/standard/45123.html
IEEE 7002	Ethical data governance in AI systems.	Global	Not certifiable; used for guidance.	https://standards.ieee.org/ieee/7002/7131/

7.4.2. Cybersecurity Standards

This table lists the cybersecurity standards in operation together with certification or conformance requirements where relevant. Certification or conformance as of May 2025 are highlighted in green.

Table 2: Cybersecurity Standards Alignment

Name	Description	Scope	Certification / Conformance	Link
NIS2 Directive	EU-wide cybersecurity directive.	EU	Oversight by national authorities; no unified certification.	https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
EU Cybersecurity Act	Cybersecurity certification framework for ICT.	EU	EU Cybersecurity Certification Framework.	https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification
Cyber Resilience Act (Proposal)	Proposed cybersecurity regulation for digital products.	EU	Via Red Alert Labs	https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

eIDAS 2.0	Secure digital identity and trust services.	EU	Trust Services Accreditation under eIDAS.	https://ec.europa.eu/digital-single-market/en/trust-services-and-eid
ISO/IEC 27001	Information Security Management standard.	Global	Certification via ISO/IEC 27006-accredited bodies.	https://www.iso.org/isoiec-27001-information-security.html
ISO/IEC 20243	Addresses threats related to maliciously tainted and counterfeit products and services.	Global	Certification via ISO/IEC 27006-accredited bodies.	https://www.iso.org/standard/74399.html
ISO/IEC 27005	Security risk management guidance.	Global	Not certifiable; supports ISO/IEC 27001.	https://www.iso.org/standard/75281.html
ISO/IEC 15408 (Common Criteria)	Standard for computer security evaluation.	Global	Certification via CCRA.	https://www.commoncriteriaportal.org/
FIDO2	Passwordless authentication protocol.	Global	FIDO Alliance Certification Program.	https://fidoalliance.org/certification/
OWASP Guidelines	Comprehensive DevSecOps framework	Global	No Certification	https://owasp.org/

7.4.3. Physical and IoT Security Standards

This table lists the physical and IoT security standards in operation together with certification or conformance requirements where relevant. Certification or conformance as of May 2025 are highlighted in green.

Table 3: Physical and IoT Security Standards

Name	Description	Scope	Certification / Conformance	Link
IEC 62443	Cybersecurity for Industrial Automation and Control Systems.	Global	Via Red Alert Labs	https://www.en-standard.eu/bs-en-iec-62443-4-2-2019-security-for-industrial-automation-and-control-systems-technical-security-requirements-for-iacs-components/?msclkid=9365827b310f12f91785ea66e6314f62

ETSI EN 303 645	Baseline requirements for consumer IoT devices.	EU	Via Red Alert Labs Conformance via ETSI TS 103 701.	https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf
ISO/IEC 27400	IoT security and privacy guidelines.	Global	Guidance only; not certifiable.	https://www.iso.org/standard/76194.html
PSA Certified	Security assurance for IoT hardware/software.	Global	Certification levels 13 available.	https://www.psacertified.org/
ISO/SAE 21434	Cybersecurity for road vehicles.	Global	Via Red Alert Labs	https://www.iso.org/standard/70918.html
PSIA	Interoperability standards for physical security systems.	Global	Conformance tools via PSIA.	https://www.psialliance.org/
FDO IoT	Device Onboarding	Global	Via Red Alert Labs	https://fidoalliance.org/certification/fido-device-onboard/
CC/EUCC	Common Criteria-based Cybersecurity Certification Scheme (EUCC	EU	Via Red Alert Labs	https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en
FIPS 104-3	Security Requirements for Cryptographic modules	USA / Canada	Via Red Alert Labs	https://csrc.nist.gov/pubs/fips/140-3/final

7.4.4. Interoperability Standards

This table lists the primary interoperability standards in operation together with certification or conformance requirements where relevant. Certification or conformance as of May 2025 are highlighted in green.

Table 4: Interoperability Standards

Name	Description	Scope	Certification / Conformance	Link
European Interoperability Framework (EIF)	Guides cross-border and cross-sector interoperability for public services.	EU	Not certifiable; provides policy and design guidance.	https://ec.europa.eu/isa2/eif_en
iSHARE Trust Framework	Framework for secure and standardised data sharing within data ecosystems.	EU / Global	Organisations undergo onboarding and certification by iSHARE Foundation.	https://www.isharefworks.org/

GAIA-X Labelling Framework	Specifies requirements for data services and interoperability compliance in GAIA-X federations.	EU	Self-assessment and third-party validation process.	https://gaia-x.eu
oneM2M Specifications (TS-0001 to TS-0008)	Standards for interoperability across IoT systems and digital twins.	Global	Test suites available via ETSI and other SDOs for conformance validation.	https://www.onem2m.org/technical/onem2m-specifications
ISO/IEC 30141	Reference architecture for IoT systems including interoperability views.	Global	Not certifiable; provides architecture guidance.	https://www.iso.org/standard/65695.html
W3C Verifiable Credentials (VC) and DID Standards	Enable decentralized identity and credential interoperability.	Global	Conformance via community-led test suites and interoperability plugfests.	https://www.w3.org/TR/vc-data-model/
OpenID for Verifiable Credentials (OpenID4VC)	Secure and interoperable exchange of verifiable credentials.	Global	Conformance testing supported by OIDF Test Suite.	https://openid.net/wg/abc/

7.4.5. Environmental Security Standards

This group of standards supports the sustainability and environmental wellbeing objectives of the 3DxVERSE and adjacent Digital Twin ecosystems.

Table 5: Environmental Security Standards

Name	Description	Scope	Certification / Conformance	Link to Certification
ISO 14001 (Environmental Management Systems)	Framework for managing and reducing environmental impacts in organisations.	Global	Certification available through ISO-accredited auditors.	https://www.iso.org/iso-14001-environmental-management.html
ISO/IEC 30145 & 30146 (Smart City ICT Framework)	Guidance on sustainable, resilient ICT architecture in smart cities and digital twin systems.	Global	Not certifiable; used for architectural and policy guidance.	https://www.iso.org/standard/53394.html
PAS 7340 (Digital Sustainability - BSI)	Framework for assessing sustainability of digital services including carbon, material, and energy use.	UK / Global	No formal certification; alignment can be demonstrated through assessment.	https://www.bsigroup.com/en-GB/standards/pas-7340/

EN 50600 (Data Centre Infrastructure Efficiency)	Defines metrics for evaluating environmental performance of data centre infrastructure.	EU	Evaluated by qualified data centre auditors.	https://www.en-standard.eu/csn-en-50600-4-3/
EU Green Digital Principles	Policy framework to support sustainable and energy-efficient digital transformation.	EU	Not certifiable; provides guidance and funding/pre-procurement criteria.	https://digital-strategy.ec.europa.eu/en/policies/european-green-digital
ITU-T L.1470 Series (ICT Sustainability Assessment)	Guidelines for measuring environmental performance of ICT infrastructure and services.	Global	Not certifiable; used for reporting and benchmarking.	https://www.itu.int/rec/T-REC-L.1470
ISO 14090 / 14091 (Climate Adaptation and Risk)	Guidance for climate risk management and adaptation planning.	Global	Used in planning; not for certification.	https://www.iso.org/standard/68507.html
WRI GHG Protocol: ICT Sector Guidance	Emissions accounting methodology for software, hardware, and ICT operations.	Global	Used for corporate carbon accounting; aligns with sustainability reporting.	https://ghgprotocol.org/ghg-sector-guidance

7.5. Trust Lists and Trust Registries

The table below lists the primary trust lists or trust registries that we will use to support trustworthy interactions and cryptographic verifiability

Table 6: Trust Lists and Trust Registries Analysis

Name	Scope	Management	API Available	Use Cases	Link
EU List of Trusted Lists (LOTL)	EU Member States' Trusted Services	European Commission	Yes	eIDAS, Digital Signatures, TSP validation	https://eidas.ec.europa.eu/efda/tl-browser/
Adobe Approved Trust List (AATL)	Global digital signature CAs	Adobe	No	PDF signing, document validation	https://helpx.adobe.com/acrobat/kb/approved-trust-list.html
Mozilla Root Store	Public CA root certificates	Mozilla	Yes (via GitHub)	SSL/TLS, email, code signing	https://wiki.mozilla.org/CA

Microsoft Trusted Root Program	Root certificates trusted by Windows	Microsoft	No (static list)	SSL, email, document security	https://learn.microsoft.com/en-us/security/trusted-root/participants-list
ICAO Public Key Directory (PKD)	Global ePassport issuing authorities	ICAO	Restricted	Border control, digital travel credentials	https://www.icao.int/Security/FAL/TRIP/Pages/PKD.aspx
EBSI Trusted Accreditation Registry	EU credential issuers and verifiers	European Commission	Yes	Cross-border public services, diplomas	https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI
eduGAIN Metadata Aggregator	Global academic federations	GANT	Yes	Federated identity, academic SSO	https://technical.edugain.org/entities
OpenID Federation	OpenID identity federations	OpenID Foundation	Yes	Federated identity, OpenID Connect	https://openid.net/specs/openid-federation-1_0.html
DIF Universal Resolver	Aggregated DIDs across methods	Decentralized Identity Foundation	Yes	Decentralized identity, DID resolution	https://uniresolver.io
Google Certificate Transparency Logs	Global issued certificates	Google	Yes	TLS monitoring, public transparency	https://www.certificate-transparency.org

7.6. Detailed roles and responsibilities in 3DxVERSE

These tables break down the different types of provider, consumer and observer roles and responsibilities together with the relevant EU frameworks that apply.

7.6.1. Providers

Table 7: Provider Roles and Responsibilities

Role	Relevant EU Frameworks	Key Responsibilities
Data Service Provider	GDPR, DGA, Data Act	Ensure lawful data collection, privacy, consent, and access conditions; may need to register as data holder under DGA.
Algorithm / Model Provider	AI Act, GDPR, Cybersecurity Act	Must classify and ensure conformity of high-risk AI systems; transparency, human oversight, fairness, explainability.

Infrastructure Provider	Cybersecurity Act, DSA, EIF	Must provide secure, trusted, and interoperable platforms; possible obligations under critical infrastructure rules.
Intermediary or Support Service Provider	DSA, GDPR	Responsible for content moderation, user access services; may be treated as intermediaries under DSA.
Orchestrator / Integrator	EIF, AI Act, DGA	Ensure semantic and technical interoperability, risk mitigation, standard adoption; enable cross-border services.

7.6.2. Consumers

Table 8: Consumer Roles and Responsibilities

Role	Relevant EU Frameworks	Key Responsibilities / Rights
Institutional / Professional User	AI Act, DGA, GDPR	Must understand and validate outputs from AI systems; benefit from data-sharing obligations under DGA.
Citizen / Community User	GDPR, DSA, AI Act	Have rights to data protection, explanation of AI decisions, access to digital public services.
Intermediary or Service Consumer	GDPR, DSA	If repackaging or re-using data/services, must comply with re-use conditions and user protections.
Innovators / Entrepreneurs	Open Data Directive, DGA, AI Act	May access high-value datasets and twin APIs; must follow AI development standards, especially for high-risk systems.

7.6.3. Observers

Table 9: Observer Roles and Responsibilities

Role	Relevant EU Frameworks	Key Responsibilities
Data Steward / Ethics & Compliance Authority	GDPR, DGA, AI Act	Ensure data minimization, lawful purpose, and explainable AI; liaise with Data Protection Officers and AI conformity assessors.
Observer (Regulators, CSOs, Auditors)	GDPR, AI Act, DSA, DGA	Monitor algorithmic fairness, privacy, access equity; ensure ecosystem transparency and citizen protections.

7.7. Detailed Functions as User Stories mapped to EU legislation and standards

Below are the functional user stories that are required to be supported mapped to EU legislation or standards. These are the 3DxVERSE Core Lifecycle that apply to all participants that will be addressed in our first iteration.

Table 10: Detailed Functions as User Stories

Function	User Story – Business Requirements	Mapped EU Legislation/Standards
Pre-Boarding / Registration		
Submit Entity Information for Evaluation	As a prospective Participant, I want to submit information about my identity, intent, capabilities, and compliance posture, so that I can be evaluated for eligibility to join the ecosystem.	eIDAS Regulation, Cybersecurity Act
Undergo Trust and Risk Assessment	As a Governance Authority, I want to evaluate the trustworthiness and risk profile of a prospective participant before allowing full participation, so that ecosystem integrity is protected.	AI Act, NIS2, Cyber Resilience Act
Consent to Baseline Governance and Legal Commitments	As a prospective Participant, I want to review and agree to the ecosystem's baseline policies, legal terms, and obligations, so that I understand the framework I'm entering.	GDPR, DSA, AI Act
Declare Intended Use Cases and Processing Activities	As a prospective Participant, I want to declare the purposes and nature of my intended activities (e.g., types of data processed, algorithms used), so that compliance and oversight requirements can be determined.	GDPR, AI Act
Provide Attestations or Certifications	As a prospective Participant, I want to submit relevant attestations, certifications, or compliance reports, so that I can demonstrate alignment with ecosystem standards.	Cybersecurity Act, AI Act
Receive Pre-boarding Status and Guidance	As a prospective Participant, I want to receive confirmation of my registration status and any guidance or next steps, so that I know how to proceed or make corrections.	EIF, Digital Principles
Participate in a Sandbox or Trial Mode	As a prospective Participant, I want to engage in a limited or sandbox mode prior to full registration, so that I can test interoperability and readiness without full commitment.	Interoperable Europe Act, AI Act (sandbox provisions)
Onboarding		
Legal and Ethical Disclosure	As a Participant, I want to understand the legal and ethical obligations before joining, so I can make an informed decision.	AI Act, GDPR

Join or Change Roles in the Ecosystem	As a Participant, I want to be able to join, move or leave roles within the 3DxVERSE ecosystem, so that I can participate in the ecosystem and make use of Digital Twin Interoperability testbed and related resources.	European Interoperability Framework (EIF), Digital Services Act (DSA)
Delegate Rights and Roles	As a Participant, I want to be able to delegate rights and roles to agents or sub-entities under my control, so that they can act on my behalf in accordance with defined scopes and responsibilities.	GDPR, eIDAS Regulation
Interoperate Across Ecosystems	As a Participant, I want to interoperate with participants from other ecosystems and trust frameworks, so that I can collaborate across domains or jurisdictions.	EIF, Data Governance Act (DGA)
Register as a Trust Authority	As an Observer, I want to register my status and scope of oversight within the ecosystem, so that I can perform governance or compliance tasks with appropriate authority and transparency.	DGA, AI Act
Define and Update Ecosystem Policies	As a Governance Authority, I want to define, update, and publish ecosystem-wide policies and operating rules, so that participants can align their activities with current legal, ethical, and technical expectations.	AI Act, Digital Governance Act
Provisioning		
Enrol and Discover Entities	As a Participant, I want to be able to enrol, make discoverable, discover or observe entities (actors, data, algorithms or services) so that I can initiate a connection to execute my use case and achieve my business objectives.	Open Data Directive, DGA
Verify Identity and Authorisation of Counterparties	As a Participant, I want to be able to verify the identity of, authenticate and authorisations of the endpoint and the counterparty behind the endpoint that I am connecting with, so that I can establish a trustworthy relationship with the counterparty.	eIDAS Regulation, Cybersecurity Act
Establish or Terminate Secure Connections	As a Participant, I want to be able to establish and terminate a secure connection between my endpoint and the endpoint of the counterparty, so that I can deliver, consume or observe the use of data, algorithms or services.	Cybersecurity Act, NIS2 Directive
Negotiate Terms of Use	As a Provider or a Consumer, I want to be able to specify, assert, change and negotiate the terms and conditions under which I will either provide, consume or observe data, algorithms or services, so that I can control my role in relation to data, algorithms or services.	DGA, DMA

Manage Consent for Personal or Sensitive Data	As a Participant, I want to be able to give, withdraw or update consent for the use of my personal or sensitive data, so that my data rights are protected.	GDPR
Register and Manage Autonomous Agents	As a Participant, I want to register and manage autonomous agents that act on my behalf in the ecosystem, so that they can securely transact or analyze data according to my policies.	AI Act, GDPR
Enable Anonymous or Pseudonymous Observation	As an Observer, I want to access audit and observability functions without revealing my identity, so that I can assess ecosystem trustworthiness without compromising safety or neutrality.	GDPR, DSA
Assign Oversight Roles	As a Governance Authority, I want to assign specific audit, monitoring, or policy enforcement roles to qualified individuals or institutions, so that governance activities can be distributed and trusted.	AI Act, DGA
Set Triggers for Oversight Actions	As a Governance Authority, I want to configure conditions under which intervention, alerts, or sanctions are triggered, so that I can automate responses to policy violations or systemic risks.	AI Act, DSA
Management		
Dynamic Risk Management	As a Participant, I want to continuously assess risks related to entities or interactions so I can take preventative measures.	AI Act, Cyber Resilience Act, NIS2
Observe, Audit, and Report on Use	As a Participant, I want to be able to observe, monitor, trace, explain, audit and report on data, algorithms and services that are provided and/or consumed so that I can prove trustworthiness and demonstrate compliance with relevant standards and legislative or regulatory requirements.	AI Act, GDPR
Track Provenance of Data and Algorithms	As a Participant, I want to access metadata about the origin, ownership, quality, and transformation history of data and algorithms, so that I can assess their reliability and ethical use.	AI Act, DGA
License or Usage Condition Tracking	As a Provider, I want to track if shared data, algorithms or services are being used under agreed licensing terms.	DGA, GDPR
Revoke or Update Access Rights and Credentials	As a Participant, I want to be able to update or revoke access rights, terminate roles, or refresh identity credentials over time, so that I can maintain control and security of my participation.	GDPR, eIDAS Regulation

Attach and Present Attestations or Certifications	As a Provider, I want to be able to attach and present attestations or certificates proving that my services or datasets comply with relevant standards and regulations, so that trust is externally verifiable.	AI Act, Cybersecurity Act
Audit Ecosystem Interactions	As an Observer, I want to monitor, trace, and audit the interactions between participants and services in real-time or retrospectively, so that I can assess alignment with trust, transparency, and ethical expectations.	DSA, AI Act
Enforce Corrective Actions	As a Governance Authority, I want to take corrective action (e.g. suspend a participant, restrict a service) in response to policy breaches, so that the integrity of the ecosystem is protected.	AI Act, DSA
Evaluate Legal Compliance	As an Observer, I want to evaluate compliance of ecosystem activities with external legal requirements (e.g. GDPR, AI Act), so that public accountability and legal conformity are ensured.	GDPR, AI Act
Enable Dispute Resolution and Redress	As a Participant, I want access to mechanisms for dispute resolution, appeal, or redress when outcomes, agreements, or services provided via the ecosystem are in conflict or breach.	DSA, GDPR
Off-boarding		
Leave the Ecosystem and Manage Data	As a Participant, I want to be able to leave the ecosystem and ensure the appropriate retention, deletion or handover of my data and digital assets, so that my exit is compliant with trust, legal, and operational obligations.	GDPR, DGA
Role Succession	As a Participant, I want to assign a successor or specify data transfer conditions before exit.	GDPR, DGA
Oversee Offboarding and Residual Risk	As a Governance Body, I want to review and oversee the termination or exit of a participant or service, so that residual risks (e.g. data retention, unresolved obligations) are assessed and managed.	GDPR, AI Act
Participant Exit Feedback	As a Governance Authority, I want to collect structured feedback from offboarding participants to improve ecosystem trust and operations.	Digital Principles
Archive Governance Evidence	As a Governance Authority, I want to archive decision logs, audit trails, and policy change history, so that I can support future transparency, accountability, and historical investigation.	DSA, DGA

7.8. Trust Frameworks Controlled Documents

Controlled documents are part of the Trust Framework. As they are listed separately, they can be updated without requiring a complete re-issuance of the overall Trust Framework.

7.8.1. Risk Management Process Summary and Risk Assessment (Aligned with ENISA Interoperable Toolbox)

The sections highlighted in green are established as a baseline in this document.

Table 11: Status against the ENISA Risk Management Process

Step	Activity	Key Toolbox Component(s)	Purpose / Notes
1	**Establish Context**	Terminology (Annex I)	Define risk scope (e.g., threat-focused or posture-focused), adopt common language.
2	**Scope Definition & Asset Identification**	Asset Classification (Annex II)	Identify primary (data/processes) and supporting assets; map local asset types to toolbox categories.
3	**Threat Identification**	Threat Taxonomy (Annex III)	Use standardized threat categories (natural, wilful, etc.); associate with affected assets and CIA triad.
4	**Define Risk Scenarios**	Terminology, Asset & Threat Mappings	Build triplets <asset, threat, impact> to describe each attack/risk scenario.
5	**Risk Assessment & Calculation**	Impact Scale (Annex IV), Probability Levels	Assess impact and likelihood per scenario using internal RM method.
6	**Risk Level Normalisation**	Risk Scale (Annex V), Mapping Libraries	Convert internal risk scores to toolbox's 5-level scale: Very Low to Very High.
7	**Risk Reporting**	Risk Level Mapping	Share normalized risk levels with stakeholders, regulators, or other orgs.
8	**Risk Treatment** *(future scope)*	*(To be developed)*	Risk treatment measures not standardized in toolbox; align with ISO/NIS2.
9	**Review & Improve**	All Components, Interoperability Libraries	Update scenarios and mappings; contribute back to toolbox evolution.

The **Risk Assessment Logs** for the programme is attached here it contains

- Project Risks, last updated 12 December 2024

- Stakeholder Risks against Trust Framework, last updated 16 April 2025
- Cybersecurity Risks, last updated 09 May 2025
- AI Risks, last updated 09 May 2025

3DxVERSE%20Risk%20Log.xlsx

7.8.2. Security Policy

7.8.2.1. Purpose and Scope

This policy establishes the principles and requirements to ensure the security of the 3DxVERSE digital twin ecosystem. It aims to safeguard the confidentiality, integrity, availability, and resilience of data, systems, and interactions across the ecosystem.

This policy applies to all participants in 3DxVERSE, including system operators, data providers, consumers, intermediaries, technology developers, and governance authorities.

7.8.2.2. Governance and Responsibility

Security within 3DxVERSE is a shared responsibility. Key roles include:

1. **Security Officers / DPOs**: Oversee policy enforcement and compliance.
2. **Node Operators**: Implement technical safeguards.
3. **Service Providers**: Embed secure-by-design practices in development.
4. **Governance Authorities**: Monitor ecosystem-wide risks and ensure accountability.
5. **Auditors / Observers**: Conduct independent oversight.

All actors must comply with applicable EU laws and international standards, including GDPR, NIS2, eIDAS 2.0, ISO/IEC 27001, and related frameworks.

7.8.2.3. Security Principles Alignment

This policy is aligned with the 3DxVERSE assurance principles:

- **Purpose-Driven Design**: Security serves the public good and protects societal and environmental wellbeing.
- **Privacy by Design**: Systems must include encryption, anonymisation, and clear consent mechanisms.
- **Secure Infrastructure**: Requires strong authentication, identity assurance, and hardened systems.
- **Resilience**: Systems must be prepared for and recover from cyberattacks, technical failure, or natural disasters.
- **Human-Centric Safety**: Participants are protected from digital harm, exclusion, or manipulation.
- **Interoperability**: Secure APIs and federated identity standards must be used.
- **Transparent Governance**: Logging and monitoring must support accountability.

7.8.2.4. Risk-Based Security Controls

7.8.2.4.1. Technical Controls

- End-to-end encryption

- Multi-factor and eIDAS-compliant authentication
- Role-based access control (RBAC)
- Certificate and key management
- Code signing for software integrity

7.8.2.4.2. Organisational Controls

- Security and privacy training
- Third-party vetting and contract clauses
- Defined security responsibilities for each role

7.8.2.4.3. Data and AI Controls

- Logging of AI decisions and training data provenance
- Prevention of data poisoning and model drift
- GDPR-compliant consent and audit trails

7.8.2.4.4. Physical and IoT Controls

- Adherence to EN 303 645, IEC 62443, and ISO/SAE 21434
- Security hardening of endpoints and devices
- Redundancy for critical assets

7.8.2.4.5. Incident Response and Recovery

- Classify incidents (e.g., breach, outage, AI failure)
- Notify affected parties within required timelines
- Maintain escalation contacts and crisis communication procedures
- Implement backup, failover, and system restoration processes

7.8.2.4.6. Compliance and Certification

Each actor must pursue appropriate certification:

- ISO/IEC 27001 for operators and IT service providers
- eIDAS-qualified Trust Services for identity providers
- FIDO2 for authentication components
- Participation in EU Cybersecurity Certification Schemes where applicable including EUCC.

7.8.2.5. Monitoring, Auditing, and Logging

Continuous monitoring of services, access, and anomalies

Immutable, role-based access to logs for governance and auditing

Log retention and tamper detection policies must be followed

7.8.2.6. Security in Development and Procurement

Secure-by-design and secure coding practices

Mandatory use of open standards and validated libraries

Procurement must prioritise security certification and open interfaces

7.8.2.7. Lifecycle Security

Onboarding: Identity verification, access provisioning

Provisioning: Secure key exchange and minimal permissions

Operation: Regular patching and threat detection

Offboarding: Credential revocation and secure data deletion

7.8.2.8. Review and Continuous Improvement

This policy will be reviewed annually or upon:

- Major regulatory changes (e.g., adoption of Cyber Resilience Act)
- Introduction of new technologies or actors
- Findings from audits or significant incidents
- Feedback is encouraged from all participants to support a living, adaptable security posture.

7.8.3. Privacy Policy

A privacy policy for citizen participants will be created based on the EU template and guidance provided by GDPR.eu. We will leverage and adapt the New Bauhaus Digital Twin Privacy Policy (Your Digital Twin is Safe!) . Accepting the privacy policy is a requirement for all citizen participants in the 3DxVERSE ecosystem and is part of the consent process in Pre-boarding/Registration.

7.8.4. Information Security Policy

Purpose: To establish a shared framework for protecting information assets across the 3DxVERSE digital twin ecosystem from unauthorized access, alteration, loss, or misuse.

Core Objectives:

- Maintain confidentiality, integrity, and availability (CIA) of systems and data.
- Secure information exchanges through encryption and mutual authentication.
- Monitor and respond to emerging threats across the digital infrastructure.

Policy Scope:

- Applies to all ecosystem participants with access to shared infrastructure or data.
- Includes technical controls, organisational controls, and third-party oversight.

Controls Framework:

- ISO/IEC 27001 (Information Security Management System)
- ISO/IEC 27005 (Risk Management)
- NIS2 Directive for operational resilience
- Access control, identity and credential management via eIDAS 2.0
- Endpoint security and secure development practices

Incident Management:

- Security incidents must be reported within 24 hours to the designated incident handler.

- Continuous logging and audit trails are mandatory for high-risk systems.

7.8.5. PLACEHOLDER Algorithmic Impact Assessment

3DxVERSE SHALL carry out an Algorithmic Impact Assessment as required in the EU Guidelines on Ethics in Artificial Intelligence and based on the Ada Lovelace Institute Algorithmic Impact Assessment Guidelines. https://www.adalovelaceinstitute.org/wp-content/uploads/2022/02/Algorithmic-impact-assessment-user-guide.pdf

7.8.6. PLACEHOLDER Data Protection Impact Assessment

3DxVERSE SHALL carry out a Data Protection Impact Assessment based on the template available at GDPR.eu. https://gdpr.eu/data-protection-impact-assessment-template/.

7.8.7. PLACEHOLDER Human Rights Impact Assessment

3DxVERSE SHALL carry out a Human Rights Impact Assessment based on the tools available from the Danish Institute for Human Rights. https://www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox/introduction-human-rights-impact-assessment

REFERENCES

[1] See Annexe EU Legislative Requirements for more details.

[2] Maple, C., Epiphanou, G., Gurukumar, N., *Facets of Trustworthiness in Digital Identity Systems,* Alan Turing Institute, May 2021. (https://www.turing.ac.uk/sites/default/files/2021-05/technical_briefing-facets_of_trustworthiness_in_digital_identity_systems.pdf) [Accessed 2 May 2025].

[3] Citiverse is a European Digital Infrastructure Consortium (EDIC) that is building an EU ecosystem of advanced AI solutions for cities. https://digital-strategy.ec.europa.eu/en/factpages/citiverse

[4] Centre of Excellence for Data Space Collaboration, Towards a Common Carrier Layer for Large-Scale Data Space Interoperability and Federation, Discussion Paper., (December 2024).

[5] Source: D4.1 V1.5 [Accessed: 2 May 2025]

[6] OWASP DevSecOps Guideline - v-0.2., https://owasp.org/www-project-devsecops-guideline/latest/ [Accessed 07 May 2025]

[7] See: https://www.esri.com/en-us/arcgis/open-vision/initiatives/standards-specifications

[8] European Open Science Cloud Association, Privacy Policy and Data Protection, see https://eosc.eu/privacy-policy/

[9] https://trustoverip.github.io/tswg-trust-registry-protocol/

[10] https://new-european-bauhaus.europa.eu/tools-and-resources/use-compass_en

[11] https://new-european-bauhaus.europa.eu/tools-and-resources/use-toolbox_en

[12]Sroor, M., Hickman, N., Kolehmainen, T., Laatikainen, G. and Abrahamsson, P., 2022. How modelling helps in developing self-sovereign identity governance framework: An experience report. *Procedia Computer Science*, 204, pp.267-277. Available at: https://doi.org/10.1016/j.procs.2022.08.032 [Accessed 16 April 2025].

[13] The EIRA© is a 5 layer reference architecture for delivering interoperable digital public services across borders and sectors.

[14] Hickman, N., et al., Overcoming Human Harm Challenges in Digital Identity Ecosystems, (November 2022) Trust over IP Foundation. [Accessed 09 May 2025]