

ToIP Governance Metamodel Specification

This is the home page for the ToIP Governance Metamodel Specification. Please see the [Governance Metamodel Companion Guide](#) for a "user's guide" to this specification. The purpose of this ToIP **specification** is to provide an overall template for ToIP-compatible **governance frameworks** from which **layer-specific templates** are derived. Each **layer-specific template** MUST comply with this specification. They SHOULD add details such as:

- Layer-specific ToIP **roles**.
- Layer-specific ToIP **processes** in which **actors** in those **roles** are engaged.
- Layer-specific **risks** against which a **risk assessment** should be performed (see the [Risk Assessment Worksheet Template](#)).
- Layer-specific elements of a **trust assurance framework** to address those **risks** (see the [Trust Assurance and Certification Controlled Document Template](#)).

Notation and Keywords

All terms appearing in **bold** on this page are listed in either the [ToIP Core Glossary](#) (based on the [ToIP Core terms wiki](#)) or the [ToIP Governance Glossary](#) (based on the [GSWG terms wiki](#).) For more information see the [Terms Wiki](#) page of the [Concepts and Terminology WG](#).

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14 \[RFC2119\] \[RFC8174\]](#) when, and only when, they appear in all capitals, as shown here.

- [Primary Document](#)
 - [Introduction](#)
 - [Terminology and Notation](#)
 - [Localization](#)
 - [Governing Authority](#)
 - [Administering Authority](#)
 - [Purpose](#)
 - [Scope](#)
 - [Objectives](#)
 - [Principles](#)
 - [General Requirements](#)
 - [Revisions](#)
 - [Extensions](#)
 - [Schedule of Controlled Documents](#)
- [Controlled Documents](#)
 - [Glossary](#)
 - [Risk Assessment](#)
 - [Trust Assurance and Certification](#)
 - [Governance Requirements](#)
 - [Business Requirements](#)
 - [Technical Requirements](#)
 - [Information Trust Requirements](#)
 - [Inclusion, Equitability, and Accessibility Requirements](#)
 - [Legal Agreements](#)

Primary Document

The **primary document** is the "home page" for the **governance framework** (GF). It:

1. MUST have a **DID** ([decentralized identifier](#)) that serves as an identifier of the entire GF.
2. MUST have a unique **DID URL** (as defined in the [W3C Decentralized Identifiers 1.0 specification](#)) to identify each specific version of the **primary document**.
3. MUST contain authoritative references to all other documents included in the GF, called **controlled documents**.

Introduction

This section is a non-normative general introduction to the GF whose purpose is to orient first-time readers as to the overall context of the GF. It:

1. SHOULD reference any external websites, white papers, or other helpful background materials.
2. SHOULD reference the [ToIP Foundation](#), the **ToIP stack**, and the specific version of the **ToIP governance template** upon which the GF is based (if any).
3. MAY include an "Acknowledgements" section citing contributors to the GF.

Terminology and Notation

This section asserts the **terminology** conventions used in the GF. It:

1. MUST explicitly specify the use of the *ToIP Governance Requirements Glossary* (see below).
2. MUST reference the GF **Glossary controlled document** for all other **terms** (see the *Controlled Documents* section).
3. MAY specify that terms specific to one **controlled document** are defined in that **controlled document**.
4. MUST specify that all RFC 2119 **keywords** used with their RFC 2119 meanings are CAPITALIZED.

5. SHOULD specify any other formatting, layout, or notation conventions used in the **primary document** and/or **controlled documents**.

ToIP Governance Requirements Glossary

requirement	In the context of a governance framework (GF), a requirement states a condition that an actor (human or machine) must meet in order to be in conformance. In ToIP-compliant GFs, all requirements MUST be expressed using RFC 2119 keywords .
mandatory	A requirement expressed using one of the following RFC 2119 keywords : "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT".
recommendation	A requirement expressed using one of the following RFC 2119 keywords : "SHOULD", "SHOULD NOT", "RECOMMENDED".
option	A requirement expressed using one of the following RFC 2119 keywords : "MAY", "OPTIONAL".
human-auditable requirement	A requirement expressed in a human language that can only be fulfilled by a human actor performing a set of processes and practices against which conformance can only be tested by an auditor of some kind. In a ToIP-compliant governance framework , human-auditable requirements are expressed as policies .
machine-testable requirement	A requirement written in a machine-readable format such that conformance of a software actor implementing the requirement can be tested by an automated test suite or rules engine . In a ToIP-compliant governance framework , machine-readable requirements are expressed as rules in a rules-based language .
policy	A human-auditable requirement that specifies some set of processes and practices that an actor must follow in order to be in conformance with the requirement .
process	A specified set of actions that an actor must take in order to be in conformance with a policy . A process may consist of a set of practices .
practice	A specified activity that an actor must perform as part of a process .
rule	A machine-testable requirement written in a machine-readable language that can be processed by a rules engine .
specification	A document or set of documents containing any combination of human-auditable requirements and machine-testable requirements needed to produce interoperability amongst implementers. Specifications may be included in (as controlled documents) or referenced from a governance framework .

Localization

This section covers the **policies** governing languages and translations for the GF. It:

1. MUST specify the official language or languages for the GF.
2. SHOULD use an [IETF BCP 47 language tag](#) to identify each official language.
3. SHOULD specify and provide links to all official translations of the GF.
4. SHOULD specify the **policies** and/or **rules** governing the production of translations.

Governing Authority

This section asserts the legal **authority** for governance of the GF.

1. For the **governing authority** (or each interdependent **governing authority**), this section:
 - a. MUST state the full legal identity including **jurisdiction(s)**.
 - b. MUST state the **DID**.
 - c. SHOULD include the [Legal Entity Identifier](#) (LEI) of the **governing authority** as defined by the [Global Legal Entity Foundation \(GLEIF\)](#).
 - d. MUST provide contact information for official communication with the **governing authority**.
 - e. SHOULD provide contact information for official persons acting on behalf of the **governing authority**.
2. For the GF itself, this section:
 - a. SHOULD provide the URL for a publicly-accessible website dedicated to the GF ("**GF website**").
3. The **GF website** SHOULD include:
 - a. HTML versions of all documents in the GF.
 - b. PDF versions of all documents in the GF.
 - c. Highlighted links to the *Governance Requirements* **controlled document(s)** that specify how the **governing authority** itself is governed.
 - d. If applicable, a primary **trust mark** displayed prominently on the home page and in the header of every other page.

Administering Authority

This section is only REQUIRED if the **administering authority** for the GF is different from the **governing authority**. It:

1. MUST state the full legal identity of the **administering authority**.
 - a. SHOULD provide the [Legal Entity Identifier](#) (LEI) of the **administering authority** as defined by the [Global Legal Entity Foundation \(GLEIF\)](#).
2. MUST provide contact information for official communication with the **administering authority**.
 - a. SHOULD provide contact information for official contacts acting on behalf of the **administering authority**.
3. MUST clearly define the **role** of the **administering authority** i.e., what administrative authority the **governing authority** delegates to the **administering authority** and what decisions and **processes** remain the responsibility of the **governing authority**.

Purpose

This is a short, clear statement of the overall purpose ("mission") of the GF. It:

1. SHOULD be as short and concise as possible—ideally one sentence, or at most one paragraph.

Scope

This is a statement of what is in and out of scope for the GF. It:

1. SHOULD clearly state the primary governed **roles** in the **trust community**.
2. SHOULD state any other relevant stakeholders.
3. SHOULD state the primary types of interactions, transactions, or **processes** in which the actors serving these **roles** will be engaged.
4. SHOULD state what kind of artifacts will be governed.
5. SHOULD, if applicable, clearly state what is out of scope.

Objectives

This section states the high-level outcomes desired by the **trust community** through its adoption of the GF. It:

1. SHOULD specify tangible, achievable results (e.g. [SMART criteria](#) and [Fit-for-Purpose criteria](#)).
2. MUST only contain outcomes over which the GF has the **authority** and mechanisms to achieve within its scope.
3. MUST be consistent with the **principles** of the GF (below).

Principles

This section states the **principles** by which all members of the **trust community** agree to abide. It:

1. SHOULD serve as a guide to the development of **policies**, **rules**, and other **requirements** in the GF ("**principles** guide **policies**").
2. SHOULD, if applicable, refer to previously existing **principles** (whether defined by ToIP or other sources).
3. SHOULD be referenced (along with any other relevant parts of the GF) in any *Legal Agreement* so as to help clarify intent.
4. MUST NOT include **requirements** (e.g., using capitalized [RFC 2119 keywords](#)) for which either human or machine conformance can be directly tested — those MUST be stated as **policies** or **rules** elsewhere in the GF.

General Requirements

This section contains **requirements** that apply to the GF as a *whole* and not just in the context of a particular **controlled document**. It:

1. SHOULD include the **requirements** that:
 - a. Generally apply to governance of the entire **trust community**.
 - b. Apply to the structure of the GF (e.g., who is responsible for which **controlled documents**).
 - c. Guide the development of more specific **requirements** within the **controlled documents**.
2. SHOULD NOT include **requirements** that apply only within the context of a specific category addressed by one of the **controlled documents**.
3. MUST include any **responsible use policies** that apply to infrastructure governed by the GF.
4. MUST include any **regulatory compliance policies** that are not specified within particular **controlled documents**.
5. SHOULD include a [Code of Conduct](#) (if not included in the legal documents) that applies to all **trust community** members.

Revisions

This section contains the specific **requirements** governing revisions to the GF. It:

1. MUST include **requirements** specifying:
 - a. How any revisions to the GF will be developed, reviewed, and approved.
 - b. How any new versions will be uniquely identified with a **DID URL**.
2. SHOULD include at least one public review period for any publicly-available GF.
3. SHOULD NOT include any other types of **requirements** that pertain to governance of the **governing authorit(ies)**. Those should be defined in **controlled documents** in the *Governance Requirements* category.

Extensions

This section applies to GFs that permit **extension GFs** (a common feature of some **ecosystem GFs**). It:

1. MUST state whether the GF can be extended.
2. MUST specify the **requirements** an **extension GF** must meet in order to be approved.
3. MUST specify the **process** by which an **extension GF** can be approved.
4. MUST define **requirements** for registration, activation, and deactivation of an approved **extension GF**.
5. MUST define the **requirements** for notification of **trust community members** about activation or deactivation of an approved **extension GF**.

Schedule of Controlled Documents

If **controlled documents** are included as part of the GF, this section **MUST** contain an authoritative list of all **controlled documents** in the GF. It:

1. **MUST** include authoritative references to all **controlled documents** in the GF.
2. **MUST** identify the exact version of each **controlled document** with a unique, permanent **DID** or **DID URL**.
3. **SHOULD** include a Web link to each **controlled documents** on the **GF website**.
4. **SHOULD** include a brief description of the purpose and scope of each **controlled document** to make it easy for readers to navigate the GF.

Controlled Documents

Each **controlled document** covers a specific area of the GF. The following sections are *categories* of **controlled documents** where each category **MAY** contain more than one document. Most (but not all) categories are **OPTIONAL**.

Glossary

This category provides a common basis for **terminology**. It:

1. **SHOULD** be a single **controlled document** for each applicable language.
2. **SHOULD** provide a common reference for all possibly ambiguous **terms** used throughout the GF.
3. **SHOULD** reference the [ToIP Core Glossary](#), other relevant ToIP **glossary** or GF-specific **glossary** for all relevant terms.
4. **SHOULD** conform to standard **requirements** for a **glossary**, i.e., list all terms alphabetically for easy reference.
5. **MAY tag** terms by category or usage.

Risk Assessment

This category includes an [ISO 27005](#) (or compatible) **risk assessment** for managing risk. **Controlled documents** in this category:

- **SHOULD** identify key **risks** that **MAY** negatively affect the achievement of the GF's purpose and **objectives** within its **scope**.
- **SHOULD** include a **risk assessment** of each key **risk** that the GF is designed to address and mitigate.
- **SHOULD** assess which **roles** and **processes** specified in the GF are vulnerable to each **risk** and what impacts could result.
- **SHOULD** include a **risk treatment plan** specifying how identified risks are to be treated (e.g. mitigated, avoided, accepted or transferred).

Trust Assurance and Certification

This category specifies **trust criteria** for **governed parties** be held accountable against **requirements** of the GF. **Controlled documents** in this category:

1. **SHOULD** include a **trust assurance framework** that defines a scheme in which **governed parties** assert compliance with the **policies** of the GF and the mechanisms of assurance over those assertions.
2. **SHOULD** (if applicable) define the roles of **auditors** and **auditor accreditors** and the **policies** governing their **actions**.
3. **SHOULD** (if applicable) define the roles of **certifying parties** and the **policies** governing their **actions** and relationships with the **governing authority, auditors** and **auditor accreditors**.
4. **SHOULD** (if applicable) include **requirements** supporting the development, licensure, and usage of one or more **trust marks**.

Governance Requirements

These are the **requirements** for governing the GF as a whole. **Controlled documents** in this category:

1. **MUST** specify governance **requirements** (e.g., Charter, Bylaws, Operating Rules, and so on) for:
 - a. The **governing authority** (or all interdependent **governing authorities**).
 - b. The **administering authority**, if applicable.
2. **SHOULD** address any **policies** required for antitrust, intellectual property rights (IPR), confidentiality, responsible use, or other **requirements** for regulatory compliance that apply to the **trust community members**.
3. **SHOULD** include any **requirements** governing enforcement of the GF and how [dispute resolution](#) will be handled.

Business Requirements

These are the **requirements** governing the business model(s) and **business rules** to be followed by the **trust community**. **Controlled documents** in this category:

1. **SHOULD** clearly explain any exchange(s) of value between **trust community members** governed by the GF.
2. **SHOULD** define the **policies** and/or **rules** governing how and when these exchanges of value take place.
3. **SHOULD** define the **requirements for the use of any decision support systems**.
4. **SHOULD** define how all **trust community members** will be held accountable for their **actions** in these exchanges.
5. **SHOULD** define how the **governing authority, administering authority**, and the GF are sustainable under these **requirements**.

Technical Requirements

These are the **requirements** governing technical interoperability. **Controlled documents** in this category:

1. MUST specify how **trust community members** will interoperate technically using the **ToIP technology stack** by reference to any relevant ToIP **s** **pecifications** and **recommendations**.
2. SHOULD include any additional **specifications** and/or **specification profiles** that are specific to the technical interoperability within this **trust community**.
3. SHOULD include references one or more **glossaries** (see *Glossary* section) as needed.
4. SHOULD reference any **test suites** or other testing **requirements**.

Information Trust Requirements

These are the **requirements** in the five categories of **trust service criteria** defined by the American Institute of Certified Public Accountants (AICPA) Assurance Services Executive Committee (ASEC). These can be addressed by implementing **internal controls** as defined by the *Committee on the Sponsoring Organizations of the Treadway Commission (COSO) Guidance on Internal Control*. **Controlled documents** in this category:

1. MUST specify the baseline **requirements** for **governed parties** with regard to:
 - a. Information security
 - b. Information availability
 - c. Information processing integrity
 - d. Information confidentiality
 - e. Information privacy
2. SHOULD specify the relevant **information trust policies** by reference to:
 - a. ToIP **specifications** and **recommendations**.
 - b. Other regulatory or industry standards.
 - c. GF-specific **policies**.
 - d. **GF-compliant decision support systems**.
 - e. **Trust community member-specific policies**.

Inclusion, Equitability, and Accessibility Requirements

These are the **requirements** governing how the GF enables fair and equal access to all. **Controlled documents** in this category:

1. MUST specify how **trust community members** will enable and promote inclusion, equitability, and accessibility by reference to:
 - a. ToIP **specifications** and **recommendations**.
 - b. Other regulatory or industry standards.
 - c. GF-specific **policies**.
 - d. **GF-compliant decision support systems**.
 - e. **Trust community member-specific policies**.
2. SHOULD specifically address how the GF is designed to help bridge (or eliminate) the **digital divide**.

Legal Agreements

This category includes any legal agreements specified in the GF. **Controlled documents** in this category:

1. MUST include all specified legal agreements between **trust community members**.
2. SHOULD reference the GF **glossary** document(s) for all **terms** not defined internally to the legal agreement.
3. MUST clearly state the **governed parties** to whom these legal agreements apply.
4. MUST define or reference all relevant accountability and enforcement mechanisms.
5. SHOULD reference any other relevant **requirements** in the balance of the GF.