ToIP Governance Metamodel

This page represents the proposed structure of the ToIP Governance Metamodel. The purpose of the metamodel is to provide an overall template for ToIP-compatible governance frameworks from which the GSWG will then develop **layer-specific templates**. Each layer-specific template will be an instance of the metamodel that adds details such as:

- Standard ToIP Roles at that layer (see the GSWG Process and Roles TF)
- Standard ToIP Processes in which actors in those roles are engaged (see the GSWG Process and Roles TF)
- Recommended Requirements for those Processes (see the GSWG Process and Roles TF)
- Standard Risks against which a Risk Assessment should be performed (see the GSWG Trust Assurance TF)
- Standard elements of a Trust Assurance Framework to address those risks (see the GSWG Trust Assurance TF)

All terms appearing in First Letter Caps on this page MUST be added to the *ToIP Glossary* tagged for inclusion in the *ToIP Governance Glossary*. (Note: the Concepts and Terminology WG has been briefed on this dependency.)

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 (defined in the DID spec) to identify each specific version of the Primary Document.
3. MUST contain authoritative references to all other documents included in the GF, called the Controlled Documents.
4. MUST include Policies in the Revisions section stating how the Controlled Documents are governed by the Governing Authority.

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 have a reference to the ToIP Foundation, the ToIP Stack, and the specific version of the ToIP Governance Template from which it was derived.
2. MAY include an "Acknowledgements" section to acknowledge the contributors to the GF.

New

Terminology

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. SHOULD specify that all RFC 2119 keywords used with their RFC 2119 meanings are capitalized.
3. MUST reference the Glossary for all other terms (see the Controlled Documents section).
4. SHOULD specify any other formatting or layout conventions used in the Primary Document or Controlled Documents.

ToIP Governance Requirements Glossary

- **Requirements** include any combination of Machine-Testable Requirements and Human-Auditable Requirements. Unless otherwise stated, all Requirements MUST be expressed as defined in RFC 2119.
    - **Mandates** are Requirements that use a MUST, MUST NOT, SHALL, SHALL NOT or REQUIRED keyword.
    - **Recommendations** are Requirements that use a SHOULD, SHOULD NOT, or RECOMMENDED keyword.
    - **Options** are Requirements that use a MAY or OPTIONAL keyword.
- **Machine-Testable Requirements** are those with which compliance can be verified using an automated test suite and appropriate scripting or testing software.
    - **Rules** are Machine-Testable Requirements that are written in a Machine-Readable language and can be processed by a Rules Engine. They are expressed in a structured rules language as specified by the GF.
- **Human-Auditable Requirements** are those with which compliance can only be verified by an audit of people, processes, and procedures.
    - **Policies** are Human-Auditable Requirements written using standard conformance terminology. For Policies using in ToIP Governance Frameworks, the standard terminology is RFC 2119 keywords. Note that all RFC 2119 keywords have weight from an auditing perspective. An implementer MUST explain why a SHOULD or RECOMMENDED requirement was not implemented and SHOULD explain why a MAY requirement was implemented.
- **Specifications** are documents containing any combination of Machine-Testable Requirements and Human-Auditable Requirements ne eded to produce technical interoperability.

Governing Authority

This section asserts the legal authority for governance of the GF. It:

1. MUST state the full legal identity of the Governing Authority or interdependent Governing Authorities.
    a. SHOULD provide an LEI for each.
2. MUST provide contact information for the Governing Authorit(ies) as Legal Entit(ies).
    a. SHOULD provide contact information for official contacts.
3. SHOULD provide a publicly-accessible Governance Framework Website (GF Website) at a URL dedicated to the GF website.
4. SHOULD include in the GF Website:
    a. If applicable, a primary Trust Mark for the GF and displayed prominently on the home page.
    b. HTML versions of all documents in the GF.
    c. PDF versions of all documents in the GF.
    d. Highlighted links to the Governance Requirements section that specify how the Governing Authority itself is governed.

Administering Authority

It the Administering Authority for the GF is different from the Governing Authority, include this section. It:

1. MUST state the full legal identity of the Administering Authority.
    a. SHOULD provide the LEI.
2. MUST state how the Governing Authority is related to and delegates administrative authority to the Administering Authority.
3. MUST provide contact information for the Administering Authority as a Legal Entity.
    a. SHOULD provide contact information for official contacts.

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 only a few sentences.

Scope

This is a statement of what is in and out of scope of 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 or transactions these Governed Roles will be engaging in.
4. SHOULD, if applicable, clearly state who and what are out of scope.

Objectives

This states the high-level outcomes desired by the Trust Community through its adoption of the Governance Framework. It:

1. SHOULD specify tangible, achievable results (e.g. SMART criteria and Fit-for-purpose criteria).
2. SHOULD specify the intended overall outcomes to be produced by conformance with the Requirements in the GF.
3. MUST only contain outcomes over which the GF has the authority and mechanisms to achieve within its Scope.
4. MUST be consistent with its Principles.

Principles

This section states the Principles by which all members of the Trust Community have agreed to abide. It:

1. SHOULD serve as a guide to the development of any Requirement based on each Principle ("Principles guide Policies").
2. SHOULD refer to existing Principles—whether defined by other ToIP GFs or by other sources—whenever possible.
3. SHOULD be referenced (along with any other relevant parts of the GF) in any Legal Agreement between Members and the Governing Authority.
4. MUST NOT include Requirements (e.g., using RFC 2119 terms) for which either human or machine conformance can be directly tested — those should be stated as Requirements 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. Apply generally to governance of the entire Trust Community;
    b. Apply to the structure of the GF, e.g., what Controlled Documents must be specified by whom and applied to whom.
    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 Responsible Use Policies that apply generally to infrastructure governed by the GF.
4. MUST include any Regulatory Compliance Policies that are not specified within particular Controlled Documents.

Revisions

This section contains the specific Requirements governing revisions to the GF. It does not include Governance Requirements for the Governing Authority or interdependent Governing Authorities (those should be defined in Controlled Documents in the **Governance Requirements** category). It:

1. MUST include Requirements specifying how any revisions to the GF will be developed, reviewed, and approved.
2. MUST include Requirements for how all new versions will be identified with a DID URL.
3. SHOULD include at least one public review period for any GF that will be available to the public.

Extensions

This section applies to GFs that permit extensions via the incorporation of other 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 Governance Framework must meet in order to be approved.
3. MUST specify the process for an Extension Governance Framework to be approved.
4. MUST define an authoritative mechanism for registration and activation of an approved Extension Governance Framework.
5. MUST define the requirements for notification of the Trust Community about an approved Extension Governance Framework.

Schedule of Controlled Documents

This is a listing 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 Document in the Web version of the GF.
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 are **categories** of Controlled Documents where each category MAY include zero or more Controlled Documents.

Glossary

The Glossary provides a common basis for terminology. It:

1. SHOULD be a single Controlled Document (even if it is organized by categories or other heuristics).
2. SHOULD provide a common reference for all possibly ambiguous terms used throughout the GF.
3. SHOULD reference the ToIP Glossary—or tagged subset(s) of the ToIP Glossary—for all terms defined there.
4. SHOULD conform to standard requirements for a glossary, i.e., list all terms alphabetically (by language) for easy reference.
5. MAY tag terms by category or usage.
6. MAY specify that terms specific to one Controlled Document are defined in that Controlled Document.

Risk Assessment

This category includes links to 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 process output that provides an assessment of each key risk that the GF is designed to address and mitigate.
- SHOULD assess which Roles and Processes are vulnerable to each risk and how they are affected.
- MAY include a Risk Treatment Plan (RTP) for how identified risks are treated (e.g. mitigated, avoided, accepted or transferred); however, all risks that are to be mitigated by Mandates in the GF SHOULD be identified.

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 document 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 directives governing their actions.
3. SHOULD (if applicable) define the roles of Certifying Parties and the requirements 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 include Controlled Documents that specify Governance requirements for the primary Governing Authority (or all interdependent Governing Authorities, or if applicable the Governing Entity), e.g., Charter, Bylaws, Operating Rules, etc.
2. SHOULD address any Antitrust Policies, Intellectual Property Rights (IPR) Policies, Confidentiality Policies, or other Requirements for regulatory compliance under which the Trust Community Members agree to operate.
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 the exchange(s) of value within the Trust Community for which the GF is designed.
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 Rules Engines or 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, Governing Entity, 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 Members of the Trust Community will interoperate technically using the ToIP Technology Stack by reference to ToIP Standard Specifications (TSS).
2. SHOULD (if necessary) reference one or more specific ToIP Interoperability Profiles (TIPs).
3. SHOULD specify any Specifications that are specific to this Trust Community.

Information Trust Requirements

These are the Requirements governing information security, privacy, availability, confidentiality and processing integrity as these terms are 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 how Members of the Trust Community will ensure the following categories of Information Trust:
    a. Information security
    b. Information privacy
    c. Information availability
    d. Information confidentiality
    e. Information processing integrity
2. SHOULD specify the relevant Information Trust Policies by reference to:
    a. ToIP Standard Specifications (TSS).

    b. Other regulatory or industry standards.
    c. GF-specific Policies.
    d. GF-compliant Rules Engines and Decision Support Systems.
    e. Trust Community Member-specific Policies.

Inclusion, Equitability, and Accessibility Requirements

These are the Policies governing how the GF enables fair and equal access to all. Controlled Documents in this category:

1. MUST specify how Members of the Trust Community will enable and promote inclusion, equitability, and accessibility by reference to:
    a. ToIP Standard Specifications (TSS).
    b. Other regulatory or industry standards/guidelines.
    c. GF-specific Policies.
    d. GF-compliant Rules Engines and Decision Support Systems.
    e. 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 or contracts included in the GF. Controlled Documents in this category:

1. MUST include all specified legal agreements or contracts between Members and/or the Governing Authority.
2. SHOULD reference the Glossary document for all terms not defined internally to the agreement or contract.
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.