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 Policies for those Processes (see the GSWG Process and Roles TF)
- Standard Risks against which 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)

The balance of this page consists of the structure of the proposed metamodel and the requirements for each component. In these requirements, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as defined in RFC 2119.

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 already been briefed on this dependency.)

- Master Document
  - Introduction
  - Purpose
  - Scope
  - Principles
  - Core Policies
  - Revisions
  - Extensions
  - Schedule of Controlled Documents

- Controlled Documents
  - Glossary
  - Risk Assessment, Trust Assurance, and Certification
  - Governance Rules
  - Business Rules
  - Technical Rules
  - Information Trust Rules
  - Inclusion, Equitability, and Accessibility Rules
  - Legal Agreements

Master Document

The Master 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 Master Document.
3. MUST contain authoritative references to all other documents included in the GF, called the Controlled Documents.
4. MUST include policies stating how the Controlled Documents are governed by the Governance Authority.

Introduction

This section is a non-normative general introduction to the GF that 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 ToIP Governance Template from which it was derived.
2. MAY include an Acknowledgements section to acknowledge the contributors to the GF.

Purpose

This is a short, clear statement of the purpose of the GF. It:

1. SHOULD be as short and concise as possible—ideally one sentence, or only a few sentences.

Scope

This is an inventory of the stakeholders, assets/artifacts and objectives for which the GF is intended to provide governance. It:

1. SHOULD clearly state the stakeholders in the Trust Community.
2. SHOULD clearly state the high-level assets/artifacts (e.g. verifiable credentials, transactions, records) under oversight by the GF.
3. SHOULD clearly state the high-level GF objectives (i.e. the desired result when the GF achieves its purpose).
4. SHOULD, if applicable, clearly state who and what are out of scope.
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 Policies based on each Principle (“Principles guide Policies”).
2. SHOULD refer to existing Principles—whether defined by ToIP-Compatible GFs or by other bodies—whenever possible.
3. SHOULD be referenced (along with any other relevant parts of the GF) in any Legal Agreement between Members and the Governance Authority.
4. SHOULD NOT include language for which conformance can be directly tested — those statements should be included as Policies.

Core Policies

This section contains the Policies that apply generally across the entire GF. It:

1. SHOULD include requirements that apply generally to governance of the entire Trust Community or that guide the development of more specific Policies within the Controlled Documents.
2. SHOULD be listed within categories to aid in understanding the context and intent of each Policy.
3. SHOULD NOT include Policies that apply in a specific category addressed by one of the Controlled Documents.
4. MUST include Responsible Use Policies that apply generally to infrastructure governed by the GF.
5. MUST include any Regulatory Compliance Policies that are not specified within particular Controlled Documents.

Revisions

This section specifies the policies for how revisions to the GF are governed. It does not include Governance Policies for the Governance Authority or interdependent Governance Authorities (those are defined in Controlled Documents in the Governance Rules category). It:

1. MUST state the full legal identity and contact information for the primary Governance Authority or interdependent Governance Authorities.
2. MUST include policies specifying how any revisions to the GF are identified, developed, reviewed, and approved.
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 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 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, Trust Assurance, and Certification

This category includes policies for managing risk, including how parties can be certified against the GF. Controlled Documents in this category:
1. SHOULD identify key risks that MAY negatively affect the achievement of the GF’s purpose within its scope
2. SHOULD include a Risk Assessment process output that provides an assessment of each key risk that the GF is designed to address and mitigate.
3. SHOULD assess which Roles and Processes are vulnerable to each risk and how they are affected.
4. SHOULD include a Risk Treatment Plan (RTP) for how identified risks are treated (e.g. mitigated, avoided, accepted or transferred).
5. SHOULD include a Trust Assurance Framework that defines how Roles assert compliance with the Policies of the GF and the mechanisms of assurance over those assertions.
6. SHOULD (if applicable) define the roles of Auditors and Auditor Accreditors and the policies governing their actions.
7. SHOULD (if applicable) define the roles of Certification Authorities and the Policies governing their actions and relationships with the Governance Authority, Auditors, and Auditor Accreditors.

 Governance Rules

These are the Rules for governing the GF as a whole. Controlled Documents in this category:

1. MUST specify the primary Governance Authority or all interdependent Governance Authorities (if any).
2. MUST include Controlled Documents that specify governance Policies for the primary Governance Authority or all interdependent Governance Authorities (e.g., Charter, Bylaws, Operating Rules, etc.)
3. SHOULD address any antitrust Policies, intellectual property rights (IPR) Policies, confidentiality Policies, or other regulatory compliance policies under which the stakeholders agree to operate.

 Business Rules

These are the Rules governing the business model(s) of the GF and/or sustainability of the Governance Authority. 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 governing how and when these exchanges of value take place.
3. SHOULD define how all Members will be accountable for their actions in these exchanges.
4. SHOULD define how the Governance Authority and the GF are sustainable under these Rules.

 Technical Rules

These are the Rules 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 technical Policies or Specifications that are specific to this Trust Community.

 Information Trust Rules

These are the Rules governing information security, privacy, availability, confidentiality and processing integrity as these terms are defined by the AICPA for service organizations. 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. Member-specific Policies.

 Inclusion, Equitability, and Accessibility Rules

These are the Rules 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. Member-specific Policies.
2. SHOULD specifically address how the GF is designed to help bridge (or eliminate) the digital divide.

 Legal Agreements

This category include any legal agreements or contracts included in the GF. Controlled Documents in this category:

1. MUST include all legal agreements or contracts between Members and/or the Governance Authority.
2. SHOULD reference the Glossary document for all terms not defined within.
3. MUST clearly state the parties to which these legal agreements apply.
4. MUST define or reference the accountability and enforcement mechanisms.
5. MUST reference any other relevant Policies in the GF.