Trust Assurance and Certification Controlled Document Template

INTERNAL REVIEW DRAFT

15 July 2021

PLEASE REVIEW IN SUGGESTING MODE. IF YOU MAKE COMMENTS, PLEASE SUGGEST EDITS TO SATISFY YOUR COMMENT

This document is being developed and approved by the
Governance Stack Trust Assurance Task Force.
The Governance Stack Trust Assurance Task Force operates within
the Trust Over IP Foundation.

Table of Contents

 PLEASE REVIEW IN SUGGESTING MODE. IF YOU MAKE COMMENTS, PLEASE SUGGEST EDITS TO SATISFY YOUR COMMENT

Author

Scott Perry, CPA, CISA - Scott S. Perry CPA, PLLC

Contributors

Line Kofoed - Bloqzone

Acknowledgements

Executive Summary

The ToIP Trust Assurance and Certification (TAC) Controlled Document Template is intended to provide a standardized structure to the Trust Assurance and Certification Controlled Document, a RECOMMENDED controlled document as specified by the ToIP Governance Metamodel Specification. The document provides RECOMMENDATIONS on what and where and when sections need to be completed as part of the controlled document section of a governance framework document. It is to be used in conjunction with the ToIP Trust Assurance Companion Guide which provides detailed guidance explaining each section and tips and techniques on their contents.

 PLEASE REVIEW IN SUGGESTING MODE. IF YOU MAKE COMMENTS, PLEASE SUGGEST EDITS TO SATISFY YOUR COMMENT

Using This Template

This document is designed to be used as a template and guide for writing a TAC or a specific governance framework. While most material in this document should be appropriate for a wide range of governance frameworks, each governance authority will need to tailor the specific content. This may involve adding and removing material from this template as needed to accommodate the needs and constraints for their particular governance framework.

To help guide the writer, there are three types of information in this Template: suggested text, fill-in fields, and instructions. A section may contain any or all these types of information.

Suggested text (plain text): Most of the document is of this type. This text has been written to use without alteration. The requirements reflect best business practice. However, the author must consider his own organization's needs, resources, and capabilities carefully to ensure that all the requirements, both those on the Issuer and on the organization itself, are adequate and can be met. Where appropriate, the suggested text can be altered, or can be replaced using the existing suggested text as an example.

Fill-in fields <in brackets>: Some sections of the document contain fields where choices must be made by the writer, to tailor it for the intended purpose. These fields are denoted by <angle brackets>, and will contain an indication of the type of information that is to be filled in. In some cases, the brackets will also contain a suggestion for the value to be filled in. The information supplied by the writer is intended to replace the fill-in field, including angle brackets.

Instruction (in talics): There are a few areas of the TAC that cannot be predicted and do not lend themselves to suggesting a generalized best practices requirement and require commentary. In this case, a paragraph will be supplied, that begins with an *Instruction: tag and is in italic typeface.* The instruction will give the writer information about how to complete the section, or by creating other documents that will be referenced. These paragraphs are intended to be removed once the TAC is completed.

Purpose

This template is intended to be used by governance architects and/or trust assurance specialists that are devising a trust assurance scheme for a governance framework. Completed documents using this template will be used by all stakeholders of a governance framework to establish and assess accountability over governance framework requirements.

 PLEASE REVIEW IN SUGGESTING MODE. IF YOU MAKE COMMENTS, PLEASE SUGGEST EDITS TO SATISFY YOUR COMMENT

1. Trust Assurance and Certification Sections

1.1 Introduction

The risk assessment process documented in the Risk Assessment Controlled Document helps to identify, analyze and treat risks germane to the governance domain. It also assesses the residual risk remaining after risk treatment.

Mandates (MUST statements) within a governance framework are intended to mitigate risk (one of the possible risk treatment options). The Trust Assurance and Certification Controlled Document is intended to convey a scheme (or framework as the terms are often used interchangeably) that holds governed parties within a governance framework accountable to its mandates. It also (depending on the rigor of the scheme) is intended to evaluate the design and operational effectiveness of the Governance Framework's mandates.

This document contains requirements for the following:

1. The Governance Framework Roles that assert and rely upon Trust
2. The set of defined Trust Criteria used in the evaluation of trust in the network
3. The Level of Assurance Relying Parties can take in the conformance of Governed Parties for processes defined within the scope of a Governance Framework
4. Types of Trust Evidence that Governed Parties produce to create assurance regarding their trust assertions
5. The Trust Assurance Process Roles that evaluate, opine, accredit and certify Trust Criteria assertion made by Governed Parties
6. Trust Assurance processes performed by Trust Assurance Process Roles.

If a Trust Assurance scheme mandates certification, consideration for the use of Trust Marks are included in this Controlled Document.

1.2 Purpose

The purpose of this document is to communicate a framework whereby stakeholders of a governance framework are held accountable to the degree warranted in mitigated risk to an acceptable residual level. Mitigation requirements are conveyed in the form of "Mandates" (MUST statements in the governance framework). This document conveys the blueprint in which governed parties provide accountability to these mandates both in design of their operations and the operational effectiveness over time.

1.3 Version

Instruction: Provide a version history of this document in this section.

1.4 Contact

Instruction: Provide contact information to the actor responsible for this document.

5 **PLEASE REVIEW IN SUGGESTING MODE. IF YOU MAKE COMMENTS, PLEASE SUGGEST EDITS TO SATISFY YOUR COMMENT**

1.5 Concepts and Terminology

1.5.1 The Concept of Trust Assurance

Within the scope of this governance framework a complete risk assessment has been completed that considers threats to the objectives of the governance framework and analyzes the likelihood and severity that will generate a qualitative impact if those threats are realized. The mandates that appear on this governance framework are required mitigations needed to reduce the risk to an acceptable level. However, risk mitigation can only occur if mandates are designed correctly, stakeholders are accountable to those mandates to the degree warranted and mitigations must be operating effectively over time.

Trust assurance in this context is a quality control measure intended to operationalize that accountability and provide a governing authority with the information needed to evaluate the design and operational effectiveness of its risk mitigation requirements. Given the numerous risks and the variety of risk mitigation controls to mitigate them, each trust assurance scheme is different.

1.5.2 The Interrelation between Trust Assurance and Risk

All governance frameworks operate within a milieu of risk. The risk assessment process is intended to consider all relevant risks and systematically analyze and triage them into a manageable set. Whereas there are a variety of risk treatment options, the main purpose of a governance framework is to convey risk mitigation requirements to reduce risk to an acceptable level (mitigations are not intended to eliminate all risk).

Relying parties of a governance framework depend on the governance framework participant's ability to mitigate risk. This is especially important for other ecosystems depending on the reliability of this governance framework to meet its stated objectives as part of a transitive trust scheme. The ability of a governance framework to hold itself accountable to its own objectives at its stated level of assurance is embodied within this document.

1.5.3 Key Terms

Instruction: Use and amend as appropriate:

- **Risk** can be defined both conceptually and operationally. ISO 31000 defines risk as the "effect of uncertainty on objectives"[1], and for organizations, it is the deviation from expected outcomes (whether positive or negative). (NIST 800-30) adopts a more traditional/operational definition of risk "a measure of the extent to which an entity is threatened by a potential circumstance or event[2]. The NIST definition is more traditional and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse

[1] https://www.iso.org/news/ref2263.html#:~:text=Risk%20is%20now%20defined%20as,on%20an%20organization's%20decision%20making. Accessed June, 2021

[2] https://csrc.nist.gov/glossary/term/risk. Accessed June, 2021

 PLEASE REVIEW IN SUGGESTING MODE. IF YOU MAKE COMMENTS, PLEASE SUGGEST EDITS TO SATISFY YOUR COMMENT

impacts to governing authority operations (i.e., mission, functions, image, or reputation), governance assets, governed parties, other organizations, and relying parties.

- **Governing Authorities** are organizations responsible for the trust of the ecosystem. They can empower governing entities to manage the ecosystem and certifying entities to convey trust.
- **Governing Parties** are organizations that define trust criteria derived from governance framework requirements that mitigate risk dealing with the security, confidentiality, availability, processing integrity and privacy of transactions. They set minimum standards for varying levels of assurance of assets that are transacted in the ecosystem. They recognize Auditor Accreditors (and issue Audit Accreditor Credentials placing them on a Credential Registry) that set rules for the qualification of auditors and audits to hold ecosystem actors accountable for these minimum standards for levels of assurance. They review governed party's performance audits and accredit them as meeting minimum standards for varying levels of assurance and issue credentials and place them on a Credential Registry so relying parties have assurance that they were issued by the stated governing party.
- **Certifying Party** - is an organization empowered to certify governed parties against a set of trust criteria. They demonstrate compliance by listing the governed party in a trust registry and/or issue them a trust mark.
- **Governed Parties** which desire to play a recognized role in an ecosystem evaluate the auditable requirements (trust criteria) from Governing Parties and implement manual, technical infrastructure and rules engine controls and credential formats to demonstrate its posture that it is compliant with that criteria. They hold themselves out to a trust assurance scheme which evaluates their criteria conformance resulting in auditor compliance reports used for continuous improvement or actions taken by governing parties to withdraw a party's right to participate in their ecosystem.
- **Audit Accreditors** develop audit standards and criteria out of governance framework requirements developed from Governing Parties. They evaluate applicant auditors for their competence, independence and quality control measures and approve them to attest to audit criteria of governed party practices. They issue compliance credentials if approved auditors can attest to audit criteria without qualification and place those credentials on credential registries.
- **Auditors** are independent professionals that are trained in evaluating technology-based evidence provided from governed parties asserting that they are in compliance with audit criteria set forth by Audit Accreditors. They issue reports attesting to their opinions which enables Governing Parties to issue compliance credentials to Governed Parties and place them on Credential Registries and add their entry to the Trust Registry.
- **Trust Registries** are repositories of Governed Parties that are recognized by a Governing Party of an Ecosystem as compliant to the trust criteria of its Governance Framework for reliance within and outside of ecosystem boundaries.
- **Credential Registries** are publicly accessible repositories of credentials issued by parties in and accessed by Verifiers during the process of validating trust. They applied Trust Assurance Criteria to the protection of Credentials in the Registry subject to audit. A Credential Registry is an optional component of the Ecosystem.

 PLEASE REVIEW IN SUGGESTING MODE. IF YOU MAKE COMMENTS, PLEASE SUGGEST EDITS TO SATISFY YOUR COMMENT

1.5.4 RFC 2119

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It has been operating since the advent of the Internet. The IETF uses Request for Comments (RFC) to convey “current best practice” to those organizations seeking its guidance for conformance purposes.

The IETF uses RFC 2119 to define keywords in their own RFCs to indicate variations in requirements. ToIP has adapted the IETF RFC 2119 for use in the Governance Metamodel, and therefore its applicable use in ToIP-compliant governance frameworks.

RFC 2119 defines keywords as they should be interpreted in the Governance Metamodel. Users of the Governance Metamodel who follow these guidelines should incorporate the following phrase near the beginning of their document:

> **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.**

RFC 2119 defines these keywords as follows:

- **MUST:** This word, or the terms "**REQUIRED**" or "**SHALL**", mean that the definition is an absolute requirement of the specification.
- **MUST NOT:** This phrase, or the phrase "**SHALL NOT**", means that the definition is an absolute prohibition of the specification.
- **SHOULD:** This word, or the adjective "**RECOMMENDED**", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT:** This phrase, or the phrase "**NOT RECOMMENDED**" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **MAY:** This word, or the adjective "**OPTIONAL**", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item.

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.

8 **PLEASE REVIEW IN SUGGESTING MODE. IF YOU MAKE COMMENTS, PLEASE SUGGEST EDITS TO SATISFY YOUR COMMENT**

An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

2. Scope

2.1 Governed Roles

Instruction: List the Roles (see scope section of the Governance Framework Scope section) of the Roles that are accountable parties to the mandates of the governance framework.

2.2 Other Relying Parties and/or Stakeholders

Instruction: List other stakeholders or other relying parties (including other ecosystems relying on transitive trust) that have a stake in this trust assurance scheme. Please see The ToIP Governance Metamodel Companion Guide - Appendix A for examples.

2.3 Governed Processes

Instruction: List the high level processes that will be in scope of this trust assurance scheme. Please see The ToIP Governance Metamodel Companion Guide - Appendix A for examples.

2.4 Artifacts

Instruction: List key components of the governance framework such as credential types, repositories and other artifacts germane to this trust assurance framework.

 PLEASE REVIEW IN SUGGESTING MODE. IF YOU MAKE COMMENTS, PLEASE SUGGEST EDITS TO SATISFY YOUR COMMENT

3. Level of Assurance

Instruction: Indicate whether and what level(s) of assurance is to be included in this trust assurance scheme. If levels are to be adopted from generally accepted standards, cite the standard(s) below.

3.1 Authoritative Source (ISO 29115, NIST 800-63-3, DIACC, eIDAS, etc.)

Instruction: Identify the source(s) of level of assurance used in the trust assurance framework. Describe how this source is used in this context.

 PLEASE REVIEW IN SUGGESTING MODE. IF YOU MAKE COMMENTS, PLEASE SUGGEST EDITS TO SATISFY YOUR COMMENT

4.1 Trust Criteria

Trust criteria is the set of mandates within a governance framework which are ascribed by governed roles within the governance framework. They comprised the set included in section 4.1 *<augmented by either jurisdictional criteria (section 4.2) and/or industry criteria (section 4.3) and/or generally accepted information trust criteria (section 4.4).>*

4.1 Governance Requirement Criteria

The set of governance criteria is derived from all governance framework mandates (MUST statements). It has been compiled into a workable set of assessable criteria in the accompanying Trust Criteria Matrix *<provide link to the separate Trust Criteria Matrix worksheet>*.

4.2 Jurisdictional Criteria

Instruction: Provide link or detail if there are jurisdictional criteria that are part of this trust assurance framework.

4.3 Industry Criteria

Instruction: Provide link or detail if there are industry criteria that are part of this trust assurance framework.

4.4 Generally Accepted Information Trust Criteria

Instruction: Provide link or detail if there are other generally accepted information trust criteria that are part of this trust assurance framework.

 PLEASE REVIEW IN SUGGESTING MODE. IF YOU MAKE COMMENTS, PLEASE SUGGEST EDITS TO SATISFY YOUR COMMENT

5. Trust Assurance Processes

5.1 Trust Assurance Scheme

Based on *<include justification for scheme>*, the following are trust scheme(s) are operating within this trust assurance framework to assure trust:

Instruction: Select from the follow (or choose another):

- ***Contracts and Agreements***
- ***Pledges***
- ***Self-Assertion***
- ***Auditor Attestation***
- ***Certification***
- ***Use of Trustmarks***

Describe the processes used to implement the scheme in this section or refer to sections within this chapter.

5.1 Trust Assurance Oversight Governance

Instruction: Describe the oversight processes that the governing or administering authority uses to ensure accountability of this trust assurance scheme. See the ToIP Trust Assurance Companion Guide for examples.

5.2 Governed Party Processes

Instruction: Describe the assertion and/or attestation processes that each set of governed parties use to ensure accountability of this trust assurance scheme.See the ToIP Trust Assurance Companion Guide for examples.

5.3 Auditor Processes

Instruction: Describe the assessment and/or attestation processes that auditors use to ensure accountability of this trust assurance scheme. See the ToIP Trust Assurance Companion Guide for examples.

5.4 Audit Accreditor Processes

Instruction: Describe the accreditation processes that audit accreditors use to ensure accountability of this trust assurance scheme. See the ToIP Trust Assurance Companion Guide for examples.

 PLEASE REVIEW IN SUGGESTING MODE. IF YOU MAKE COMMENTS, PLEASE SUGGEST EDITS TO SATISFY YOUR COMMENT

5.5 Certification Body Processes

Instruction: Describe the certification processes that certification bodies use to ensure accountability of this trust assurance scheme. See the ToIP Trust Assurance Companion Guide for examples.

5.6 Trust Mark Processes

Instruction: Describe the set of trust mark processes that enable the use of trust marks within this trust assurance scheme. See the ToIP Trust Assurance Companion Guide for examples.