Trust Criteria Matrix Companion Guide

Version 1.0
19 October 2021

This publicly available guide was approved by the ToIP Foundation Steering Committee on 19 October 2021.

The mission of the Trust over IP (ToIP) Foundation is to define a complete architecture for Internet-scale digital trust that combines cryptographic assurance at the machine layer with human accountability at the business, legal, and social layers. Founded in May 2020 as a non-profit hosted by the Linux Foundation, the ToIP Foundation has over 300 organizational and 100 individual members from around the world.

Please see the end page for licensing information and how to get involved with the Trust Over IP Foundation.

Table of Contents

Document Information

Author

Scott Perry — Scott S. Perry CPA PLLC

Contributors

Line Kofoed — Sovrin
Sankarshan Mukhopadhyay — Sovrin
Karen Hand — Precision Strategic Solutions

Acknowledgements

The Trust over IP Trust Assurance Criteria Matrix Template contains structural elements from the Sovrin Trust Assurance Matrix V3 that were developed by Line Kofoed and Sankarshan Mukhopadhyay in the Sovrin Governance Framework Working Group and were contributed to the Trust Over IP Foundation under the CC BY-SA 4.0 licence

Revision History

Version	Date Approved	Revisions
1.0	19 October 2021	Initial Publication

Terms of Use

THESE MATERIALS ARE PROVIDED “AS IS.” The Trust Over IP Foundation, established as the Joint Development Foundation Projects, LLC, Trust Over IP Foundation Series ("ToIP"), and its members and contributors (each of ToIP, its members and contributors, a "ToIP Party") expressly disclaim any warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to the materials. The entire risk as to implementing or otherwise using the materials is assumed by the implementer and user.

IN NO EVENT WILL ANY ToIP PARTY BE LIABLE TO ANY OTHER PARTY FOR LOST PROFITS OR ANY FORM OF INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER FROM ANY CAUSES OF ACTION OF ANY KIND WITH RESPECT TO THESE MATERIALS, ANY DELIVERABLE OR THE ToIP GOVERNING AGREEMENT, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, AND WHETHER OR NOT THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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 to ensure maximal efficiency in operation. IETF has been operating since the advent of the Internet using a 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 for use in RFC documents; these keywords are used to signify applicability requirements. ToIP has adapted the IETF RFC 2119 for use in the <name of this document>, and therefore its applicable use in ToIP-compliant governance frameworks.

The RFC 2119[1] keyword definitions and interpretation have been adopted. Those users 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.

[1] https://datatracker.ietf.org/doc/html/rfc2119. Accessed June 2021.

An implementation which does not include a particular option MUST be prepared to interoperate with other implementations which include the option, recognizing the potential for reduced functionality. As well, implementations which include a particular option MUST be prepared to interoperate with implementations which do not include the option and the subsequent lack of function the feature provides.

Executive Summary

The Trust over IP (ToIP) Criteria Matrix Companion Guide (TCMCG) and Template serve as a blueprint for governing authorities to construct an operational depiction of how to implement a trust assurance framework - specifically, how to hold governed parties accountable to the mandates (MUST statements) within a governance framework. The trust assurance framework specifies the degree it will hold governed parties accountable and the governed roles it requires to participate in the scheme. The set of mandates constitute the 'trust criteria' of the governance and trust assurance frameworks. Trust criteria need to be communicated to governed parties and those involved in trust assurance (e.g., auditors, accreditors, and certifiers) ensuring transparent accountability, consistency and fairness to all parties.

The TCMCG describes the development and operational processes used in creating and deploying trust criteria according to the standards set forth in the Trust Assurance and Certification Controlled Document of the governance framework. It is intended to be used in conjunction with the ToIP Trust Criteria Matrix (TCMT) Template so governance architects can build trust criteria that aligns specifically to their governance framework.

Introduction

The Trust over IP Foundation (ToIP), by defining a complete architecture for Internet-scale digital trust, seeks to enable trusted ecosystems comprised of individuals and organizations - to leverage collective intelligence and expertise, enable innovative business opportunities, and innovative solutions to societal challenges related to our environment, health, productivity, and resource allocation. To succeed, emerging ecosystems require governance authorities and a robust governance framework to identify and mitigate risks with the potential to harm individuals, the organizations, and the overall well-being of the network.

An important component of any trust assurance framework is the operational actions that are required to hold governed parties accountable to the mandates (MUST statements) within a governance framework. The trust assurance framework specifies the degree it will hold governed parties accountable and the governed roles it requires to participate in the scheme. The set of mandates constitute the 'trust criteria' of the governance and trust assurance frameworks. Trust criteria needs to be communicated to governed parties and those involved in trust assurance (e.g., auditors, accreditors and certifiers) so that accountability can be transparent, consistent and fair to all parties.

The Trust over IP (ToIP) Criteria Matrix Companion Guide (TCMCG) describes the development and operational processes used in creating and deploying trust criteria according to the standards set forth in the Trust Assurance and Certification Controlled Document of the governance framework. It is intended to be used in conjunction with the ToIP Trust Criteria Matrix Template (TCMT) so governance architects can build trust criteria that aligns specifically to the governance framework.

This guide is not intended to replace other generally accepted trust criteria derived from marketplace standards. These standards will be useful in complementing the mandates within the governance framework. This guide assists architects in deriving trust criteria where there are no other generally accepted standards; typically, when the governance framework includes very specific and tailored mandates for its purposes.

Purpose

This guide provides emerging ecosystems, organizations, and individuals with the guidance to compile and issue a set of criteria that SHOULD hold governed parties accountable to the degree set forth in the governance framework's trust assurance scheme. It is intended to serve a diverse group of professionals including:

- Architects of governance frameworks,
- Governing authority leaders,
- Functional governed party leaders with responsibilities for conducting organizational missions/business functions (e.g., mission/business owners, information owners/stewards, authorizing officials),
- Individuals with responsibilities for acquiring information technology products, services, or information systems (e.g., acquisition officials, procurement officers, contracting officers),

- Individuals with information system/security design, development, and implementation responsibilities (e.g., program managers, enterprise architects, information security architects, information system/security engineers, information systems integrators),
- Individuals with information security oversight, management, and operational responsibilities (e.g., chief information officers, senior information security officers, information security managers, information system owners, common control providers), and
- Individuals with information security/risk assessment and monitoring responsibilities (e.g., system evaluators, penetration testers, security control assessors, risk assessors, independent verifiers/validators, inspectors general, auditors).

Trust assurance criteria conveys the set of accountable mandates required by governed participants in a governance framework. It communicates specific requirements to roles and holds them accountable to the degree specified within a trust assurance framework. This guide and associated Trust Criteria Matrix Template provide governance architects the methods to develop and execute transparent, consistent, fair accountability of its governance framework. It is flexible to accommodate levels of accountability from simple pledges to compliance through to complex certification schemes and offers recommendations for operational deployment and continual improvement.

1. The Purpose of Trust Assurance Criteria

Governing authorities operate through stated requirements. Jurisdictions have laws, games have rules, and companies have bylaws, charters, policies, practices and processes that are expected to be consistently followed. This set of requirements need to be transparent, consistent, and fair in order for them to be effortlessly and consistently followed. Roles and actors that participate in a governance framework need to clearly understand the requirements in order to make uncoerced decisions regarding the risks, costs and benefits of participating in a governance framework.

Governance requirements and trust assurance criteria are directly aligned. Trust assurance criteria is the set of mandates (MUST statements from the governance framework) that the governing authority wants governed parties to hold themselves accountable to the degree set forth in its trust assurance scheme. As stated in the ToIP Trust Assurance Companion Guide, a trust assurance scheme can range from a simple pledge that governed parties will conform to governance framework requirements to a highly complex certification scheme driven by a recognized certification body.

The purpose of trust assurance criteria is to operationalize accountability of governance requirements.

1.1 Concepts and Terminology

A **trust criteria matrix** is a published set of governance mandates intended to operationalize compliance to the degree published by a trust assurance framework within a governance framework.

Governed role control practices are specific activities performed by governed roles of a governance framework designed to ensure that governance requirements are met.

Control activities are the policies, procedures, techniques, and mechanisms that help ensure that management's response to reduce risks identified during the risk assessment process is carried out. In other words, control activities are actions taken to minimize risk.

COBIT (Control Objectives for IT) is a framework for the governance and management of enterprise information and technology, aimed at the entire enterprise. COBIT defines the components and design factors to build and sustain a best-fit governance system. The globally recognized COBIT® 2019 Framework2 helps ensure effective EGIT, facilitating easier, tailored implementation—strengthening COBIT's continuing role as an important driver of innovation and business transformation.

Computer-assisted audit tool (CAAT) or computer-assisted audit tools and techniques (CAATs) is the practice of using computers to automate the IT audit processes. CAATs normally include the use of basic office productivity software such as spreadsheet, word processors and text editing programs

[2] https://www.isaca.org/resources/cobit

and more advanced software packages involving statistical analysis and business intelligence tools. Dedicated specialized software are also available (see below). CAATs have become synonymous with data analytics in the audit process.

Audit sampling is an investigative tool in which a finite number of samples (items) are chosen (haphazardly or systematically) from the entirety from a given population to be audited. It is an auditing technique that provides supporting evidence that allows auditors to issue audit opinions without having to audit every single item and transaction.

2. Trust Criteria Matrix Lifecycle

ToIP RECOMMENDS the following process for development and deployment of a trust criteria matrix:

1. Inventory Governance Framework Mandates
2. Categorize Governed Roles and ToIP Stack Levels
3. Develop Suggested Control Practices
4. Identify Evidence
5. Establish Suggested Audit Techniques (If applicable)
6. Test the Scheme
7. Feedback and Continuous Improvement

2.1 Phase 1 - Inventory Governance Framework Mandates

The first step in trust criteria creation is the gathering of all governance framework MUST mandates (as opposed to SHOULD or MAY), as MUST mandates are always required and carry the consistent accountability that a trust assurance scheme needs to be robust. Inclusion of SHOULD requirements and related conditions would create challenges for effective trust criteria management.

Furthermore, not all MUST mandates need to be included in the trust criteria. Some MUST mandates may not carry the accountability aspect of governed roles to enable it to be useful in a trust assurance scheme; for example, high-level requirements or those not tied to a specific governed role.

Where are the governance mandates? They are included in most sections of the governance framework, from the Primary Document to the set of Controlled Documents that are part of the Governance Framework set. They may also be found as a set of requirements found in a reference link from a governance framework document. It is RECOMMENDED to do a thorough search of governance MUST mandates to ensure that all are captured.

All selected governance framework MUST mandates are brought into the associated Trust Criteria Matrix Template (TCMT) by a simple cut and paste into Column D of the template. A unique reference number should be tagged to each mandate in Column C. Typically, up to a three letter acronym of the source of the mandate (e.g., GPD for Governance Primary Document) followed by an index number is RECOMMENDED so there is always a direct link between the trust criteria and the governance framework.

2.2 Phase 2 - Categorize Governed Roles and ToIP Stack Levels

After adding the governance framework MUST mandates into the trust criteria template, the next step is to categorize the mandates into ToIP stack levels and governed roles.

ToIP governance frameworks transcend all layers of the ToIP stack. In the event where all governed roles occur within one layer of the ToIP stack, inclusion of column A in the TCMT may not seem necessary; however, to provide for future flexibility consider its inclusion. When an ecosystem governance framework involves multiple stack layers, column A provides helpful information regarding the stack layer delineation.

For operational clarity, every governed role should be provided a list of role-assigned trust criteria requirements. However, to optimize accountability it is RECOMMENDED that all trust criteria requirements that are attributed to more than one role be attributed to each role specifically in the matrix showing a duplicate entry per role. The TCMT includes a Roles tab with suggested acronyms for many of the governed party roles that can be used and/or modified as needed. Alternatively, a new set of acronyms can be employed. With filtering capacity attached to Column B, one can easily generate a list of trust criteria requirements on a per role basis.

2.3 Phase 3 - Develop Suggested Control Practices

Governance requirements convey a set of expected warranted results from the governed parties. It does not specify the details on how that result are achieved. Control practices are the set of activities under control of a governed party that can be deployed to achieve a governance mandate. Control activities include a variety of mechanisms, techniques, policies, procedures, techniques, and mechanisms under the control of a governed party that contribute to the achievement of the control practices.

Within a trust assurance scheme, control activities need to be designed to achieve governance mandates at any point of time and be operational effective over recurring periods of time (typically a year).

While governed parties will personalize specific control practices tailored to their specific environments, they need guidance in the form of the trust matrix to demonstrate acceptable examples of control practices designed to achieve governance mandates. This is the information needed to populate Column E of the TCMT.

More than one control practice is often needed to achieve any one specific governance mandate. The control practices required for a specified mandate need to be uniquely recorded in the TCMT (i.e., separate row per practice - potentially using the “row merge ’’feature of spreadsheet software, by mandate).

What are examples of control practices? Given the wide breadth of potential governance framework mandates that could be included in trust criteria, it would be difficult to provide a one-size-fits-all blueprint. However, as mentioned above, the globally recognized ISACA organization COBIT has established a comprehensive framework consisting of a set of control objectives and control practices for the governance and management of enterprise information and technology. COBIT defines the components and design factors to build and sustain a best-fit governance system.

COBIT is a proprietary framework available free to all members of ISACA (for a fee for non-members). It provides a robust catalogue of control objectives (which can be matched to governance framework mandates) and the associated control practices that are designed to achieve them. ToIP RECOMMENDS using COBIT as a guide for developing suggested control practices to meet governance framework mandates.

When publishing control practices in the TCMT (i.e., a row), each practice should be assigned a unique control practice identifier (ID in Column F) for the purpose of managing linkages and cross references.

2.4 Phase 4 - Identify Evidence

A critical step for governed parties to assert/support their compliance in meeting governance mandates is the presentation of evidence to governing/administering authorities, auditors or certifying parties. As stated in the ToIP Trust Assurance Companion Guide, trust assertions are empty without evidence to support it. The evidence presented must be sufficient, appropriate, and persuasive to be effective. The TCMCG identifies a wide array of example evidence sets that can be included in Column G of the TCMT.

Not all evidence supporting governed party assertions will be in the form of digital artifacts (e.g., document, screenshot, diagram, configuration setting, etc.). Evidence demonstration might require a walkthrough of controls to demonstrate a functioning and consistent process. When no tangible evidence can be defined or demonstrated, the least persuasive but acceptable verification of evidence could include a corroborate inquiry of multiple control owners (for further discussion refer to Section 3.5).

2.5 Phase 5 - Establish Suggested Audit Techniques (If applicable)

If the trust assurance scheme requires the involvement of independent auditors or certifying parties, then Column H of the TCMT MUST be completed for each control practice listed in Column E.

There are five main methods to walk through and test a control practice assigned to a governed party. These methods include (listed in order of complexity from lowest to highest): inquiry, observation, examination or inspection of evidence, re-performance, and computer assisted audit technique (CAAT)3.

- Inquiry: Simply, the auditor asks questions concerning control practices to appropriate organization members (e.g., management or employees) concerning the controls in place to collect relevant information. This method is often used in conjunction with inquiry with multiple parties (i.e., corroborative inquiry) and other methods outlined above. For example, an auditor may inquire of management if visitors to the data center are escorted at all times in the event

[3] https://linfordco.com/blog/audit-procedures-testing/

an auditor is not able to observe this activity while on site. No control practice or criteria should ever be supported by controls only tested through single inquiry procedures as it presents the least persuasive form of evidence.

- Observation: Activities and operations are tested using observation. This method is useful when there is no documentation of the control operation or activity, for example, observing that a security camera is in place, or a fire suppression system is installed.
- Examination or Inspection of Evidence: This method is used to determine whether manual controls are being performed. For instance, backups scheduled to run on a regular basis or the correct filling of required forms. This method often includes reviewing the written documentation and records (e.g., employee manuals, visitor logs, and system databases).
- Re-performance: Re-performance (sometimes called recalculation) is used when the above three methods combined fail to provide sufficient assurance that a control is operating effectively. This method can also be used to provide independent demonstration that controls are operating effectively. This method of testing (as well as a CAAT) provides the **strongest** evidence concerning the operating effectiveness of a control. Re-performance requires the auditor to manually execute the control, such as re-performing a calculation to confirm an automated system performs the control calculation correctly.
- CAAT: This method can be used to analyze large volumes of data, providing the ability to analyze all transactions (as opposed to a finite sample). A CAAT analysis usually requires the use of software ranging from simple spreadsheets to specialized databases or analytical software designed specifically for data analytics (e.g., ACL).

Audit sampling (auditing a finite sample of activities) is an acceptable audit method used to generate insight concerning the entirety of the control activities. Various sampling strategies (e.g., stratification - sampling within identified subpopulations) provide effective means for controlling selection bias and minimizing error. Two of the most common sampling strategies include simple random sampling or a skewed bias sample when there are inherent differences in variability or bias among groups within a population.

Section 3.4 of the COBIT Framework provides an extensive reference for the design of audit procedures (including a number of examples).

2.6 Phase 6 - Test the Scheme

At the testing stage, a completed matrix has been developed but it is not known how effective it is in achieving the accountability objectives of the trust assurance framework. Testing is required to identify issues in control design and its operating effectiveness. This requires a fulsome evaluation of the matrix undertaken by stakeholders acting as beta testers to evaluate wording, applicability, efficiency and effectiveness against its defined objectives.

There SHOULD be an evaluation of test results and a mechanism for updating and finalizing the trust criteria matrix.

2.7 Phase 7 - Feedback and Continuous Improvement

At some point, the Trust Criteria Matrix will become available to governed parties to use. Most trust assurance schemes involve an initial design review of the criteria followed by a period (up to a year) review of operating effectiveness of the governed party's conformance. Annual reviews will solicit feedback and improvement recommendations of the trust matrix content.

Concluding Summary

The Trust over IP Foundation (ToIP), by defining a complete architecture for Internet-scale digital trust, seeks to enable trusted ecosystems. Ecosystems require governance authorities and a robust governance framework.

A trust assurance framework is a mechanism to hold governed parties accountable to the mandates (MUST statements) within a governance framework. The trust assurance framework specifies the degree it will hold governed parties accountable and the governed roles it requires to participate in the scheme. The set of mandates constitute the ‘trust criteria’ of the governance and trust assurance frameworks. Trust criteria needs to be communicated to governed parties and those involved in trust assurance (e.g., auditors, accreditors and certifiers) so that accountability can be transparent, consistent and fair to all parties.

The ToIP Trust Assurance Companion Guide (TACG) provides an architectural blueprint for developing a trust assurance framework. The TCMCG provides guidance for the development and operational processes used in creating and deploying trust criteria according to the standards set forth in the Trust Assurance and Certification Controlled Document of the governance framework. It is intended to be used in conjunction with the ToIP Trust Criteria Matrix Template (TCMT), a tool for governance architects to build trust criteria that aligns with the mandates outlined by the governance framework.

The Trust Over IP Foundation (ToIP) is hosted by the Linux Foundation under its Joint Development Foundation legal structure. We produce a wide range of tools and deliverables organized into five categories:

- Specifications to be implemented in code
- Recommendations to be followed in practice
- Guides to be executed in operation
- White Papers to assist in decision making
- Glossaries to be incorporated in other documents

ToIP is a membership organization with three classes—Contributor, General, and Steering.

The work of the Foundation all takes place in Working Groups, within which there are Task Forces self-organized around specific interests. All ToIP members regardless of membership class may participate in all ToIP Working Groups and Task Forces.

When you join ToIP, you are joining a community of individuals and organizations committed to solving the toughest technical and human centric problems of digital trust. Your involvement will shape the future of how trust is managed across the Internet, in commerce, and throughout our digital lives. The benefits of joining our collaborative community are that together we can tackle issues that no single organization, governmental jurisdiction, or project ecosystem can solve by themselves. The results are lower costs for security, privacy, and compliance; dramatically improved customer experience, accelerated digital transformation, and simplified cross-system integration.

To learn more about the Trust Over IP Foundation please visit our website, https://trustoverip.org.

Licensing Information:
All Trust Over IP Foundation deliverables are published under the following licenses:

Copyright mode: Creative Commons Attribution 4.0 International licenses
http://creativecommons.org/licenses/by/4.0/legalcode

Patent mode: W3C Mode (based on the W3C Patent Policy)
http://www.w3.org/Consortium/Patent-Policy-20040205

Source code: Apache 2.0.
http://www.apache.org/licenses/LICENSE-2.0.htm