Sovrin Trust Assurance Framework V1

2019-03-27

sovrin

identity for all

Introduction

A primary purpose of the Sovrin Foundation is to address increasing concerns about security and privacy on the Internet, particularly with respect to digital identity. These concerns have resulted in diminished public trust in the Internet as a global public utility, which in turn has eroded our collective ability to harness the Internet's power for economic and social empowerment and digital transformation.

For the Sovrin Network itself to be trusted as a global public utility, the public must be able to assess the degree to which the providers of Sovrin Infrastructure, including the Sovrin Foundation, Stewards, Agencies, and Developers, comply with the policies specified in the Sovrin Governance Framework. This is the purpose of the Sovrin Trust Assurance Framework.

Versioning

The Level of Assurance that can be asserted by the Sovrin Governance Framework will evolve over time depending on a number of factors including:

- Operational network roles
- Inherent risk in the network
- Risk management measures taken by roles in the network
- Complexity of transactions
- The level of automated controls
- The level of governance in place
- The role of trust actors in the network

Each version of this document is tied to the Sovrin Governance Framework at a specific point of time. See the revision dates of this document and of the referenced documents in the Sovrin Governance Framework to clarify the current state.

The Sovrin Ledger initially went live on 31 July 2017, when the Sovrin Foundation created the Genesis Transactions with six Sovrin Trustees and ten Stewards. From that point until the approval of the Sovrin Governance Framework V2 on 27 March 2018, all active Stewards had executed the Sovrin Founding Steward Agreement. Under the Sovrin Governance Framework V2, all Stewards must execute the Sovrin Steward Agreement.

In the Sovrin Governance Framework, the Sovrin Foundation has established a Self-Certification Policy for all active Stewards.

This version of this document will only convey operational components.

Terminology

All terms in First Letter Capitals that are not defined in this document (as called out in a specific section) are defined in the Sovrin Glossary.

1. Purpose

The purpose of the Sovrin Trust Assurance Framework is to identify:

1. The Trust Elements (defined in Section 3) that Trust Actors (defined in Section 7) assert in the Sovrin Network.
2. The Sovrin Ledger Roles (Section 4) that assert and rely upon trust.
3. Generally-Accepted, Sovrin-Specific, or Domain-Specific Trust Criteria used in the evaluation of trust in the Sovrin Network (defined in Section 5).
4. The Trust Assertions that Sovrin Ledger Roles make against Trust Criteria (defined in Section 5).
5. The Trust Evidence that Trust Actors produce to create assurance regarding their trust assertions (defined in Section 6).
6. The Trust Mechanisms in place to assert and evaluate trust (defined in Section 8).
7. The process of Trust Governance whereby trust assertions are evaluated and deemed trustworthy, so they can be relied upon by Relying Parties (defined in Section 9).

2. Level of Assurance

This document describes the Level of Assurance a Relying Party can derive from the Sovrin Governance Framework. This section defines the maximum level.

The Sovrin Governance Framework claims a **maximum** level of a **reasonable** Level of Assurance.

In May 2013, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) updated its Internal Control—Integrated Framework (the original framework). The original framework has gained broad acceptance and is widely used around the world. It is recognized as a leading framework for designing, implementing, and conducting internal control and assessing the effectiveness of internal control. Internal control is defined as follows:

> *Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.*

This definition reflects certain fundamental concepts. Internal control is:

- Geared to the achievement of objectives in one or more categories—operations, reporting, and compliance
- A process consisting of ongoing tasks and activities—a means to an end, not an end in itself
- Effected by people—not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to affect internal control
- Able to provide reasonable assurance—but not absolute assurance, to an entity's senior management and board of directors
- Adaptable to the entity structure—flexible in application for the entire entity or for a particular subsidiary, division, operating unit, or business process

This definition is intentionally broad. It captures important concepts fundamental to how organizations design, implement, and conduct internal control, providing a basis for application across organizations that operate in different entity structures, industries, and geographic regions.

The ICAEW definition of a reasonable assurance audit engagement is:

> *Where the practitioner needs to reduce the assurance engagement risk (the risk that an inappropriate conclusion is expressed when the information on the subject matter is materially misstated) to an acceptably low level as the basis for a positive form of expression of the practitioner's conclusion. Such risk is never reduced to nil and therefore, there can never be absolute assurance.*

Per the ICAEW guidance on management of risk and liability, relying parties may perceive less than reasonable assurance based on their evaluation of the Sovrin Governance Framework and the Sovrin Trust Assurance Framework but not more.

3. Trust Elements

The following Trust Elements guide the development of specific Trust Criteria asserted by Trust Actors in the Sovrin Network. These are based on the AICPA Trust Services Criteria based on COSO Internal Control - Integrated Framework, for use in attestation or consulting engagements to evaluate and report on controls over information and systems (a) across an entire entity; (b) at a subsidiary, division, or operating unit level; (c) within a function relevant to the entity's operational, reporting, or compliance objectives; or (d) for a particular type of information used by the entity.

- ***Security***. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

- ***Availability***. Information and systems are available for operation and used to meet the entity's objectives.
- ***Processing integrity***. System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- ***Confidentiality***. Information designated as confidential is protected to meet the entity's objectives.
- ***Privacy***. Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

4. Sovrin Roles Making Trust Assertions

The following Sovrin Ledger Roles make Trust Assertions with regard to the Trust Elements to Relying Parties within the Sovrin Community:

1. Sovrin Foundation (including the Sovrin Board of Trustees).
2. Steward.

5. Trust Criteria

5.1 Sovrin-Specific Trust Criteria

For the Sovrin Governance Framework V2, the only Trust Criteria in operation are self-developed by the Sovrin Foundation and appear in section 10 and in an Addendum to that document. It comprises governance Policies the Sovrin Foundation has set for itself and the Steward Business Policies and Steward Technical Policies it mandates for Stewards.

6. Trust Evidence

Trust assertions are empty without evidence to support it. The following are examples of Trust Evidence that are used to support Trust Assertions for the Sovrin Governance Framework V2.

1. Signed Contracts.
2. Signed Agreements.
3. Configurations.
4. Signed Approvals.
5. Policies.
6. Procedures.
7. Logs.

    a. Security.
    b. Application.
    c. System.
    d. Database.
8. Incident Records.

For the Sovrin Governance Framework V2, see the Trust Assurance Matrix (Addendum) for the specific Trust Evidence used in this version of the Sovrin Trust Assurance Framework.

7. Trust Actors

The following is the set of Sovrin Entities who play a role in the Sovrin Governance Framework V2 in assessing and opining on Trust Assertions in the Sovrin Network.

1. **Sovrin Board of Trustees**. Issues the Policies within the Sovrin Governance Framework and has the right to approve and suspend Stewards from the Sovrin Network. It has the right to perform Self-Certification to evoke assurance from Relying Parties.
2. **Stewards**. Agree to the Sovrin Steward Agreement and perform Self-Certification of compliance with the Steward Business Policies and Steward Technical Policies.
3. **Legal Authorities**. Enforce laws in the Jurisdictions of the Sovrin Foundation and Stewards and mediates the Sovrin Steward Agreement if challenged.

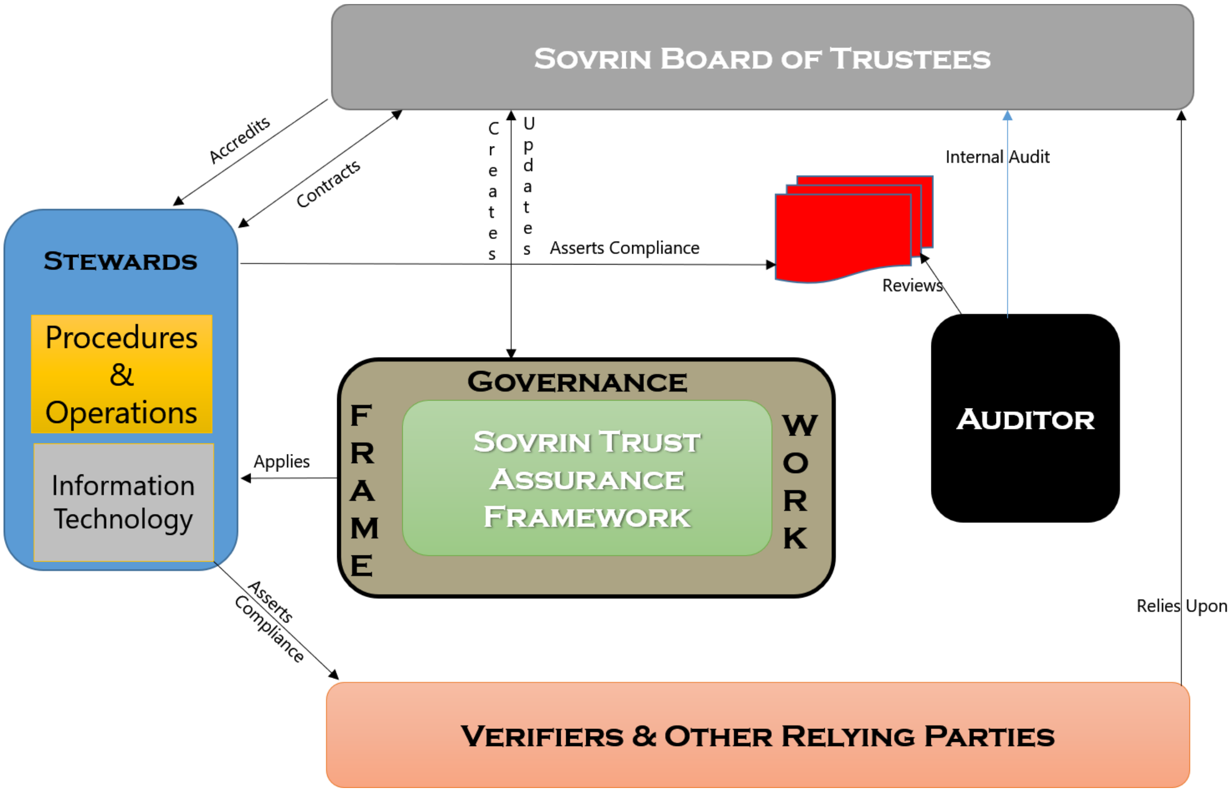
8. Trust Mechanisms

The following are actions that the Sovrin Foundation takes to assert and assure trust:

1. Contracts and Agreements.
2. Self-Assertion.
    a. Sovrin Trust Criteria Compliance.
    b. Legal Compliance.

9. Trust Governance

The following is a graphical and procedural depiction on how trust asserted from Sovrin Ledger Roles are currently received, assessed, and relied upon in the Sovrin Network.



For the Sovrin Governance Framework V2:

1. The Sovrin Board of Trustees has established the Sovrin Governance Framework and this Sovrin Trust Assurance Framework. It has created its own Policies and those it requires of Stewards in their Sovrin Ledger Role in the Sovrin Network.
2. The Sovrin Board of Trustees requires Stewards to sign the Sovrin Steward Agreement and perform Self-Certification that the Steward is compliant with the *Steward Business Policies* and the *Steward Technical Policies*. This Self-Certification is reviewed by the responsible Sovrin Governing Body and reported to the Sovrin Board of Trustees prior to approval of the Steward.

10. Trust Assurance Matrix

The Sovrin Trust Assurance Matrix is a tabbed spreadsheet which correlates existing Sovrin Governance Framework Policy statements across Sovrin Governance Framework V2 documents and relevant stakeholders. This matrix is the foundation of self and third-party audits needed to verify compliance to the Sovrin Governance Framework.