# Identity Utility Network for Business

## Disclaimer

The content presented herein is offered as a discussion starter.

All names and pricing are offered for conceptual purposes and should not be considered final.

## Purpose

Establish a consortium along with a governance framework for a decentralized identity utility that businesses can comfortably participate in and reliably use.

## Audience

This proposal is intended as a discussion starter for Sovrin Foundation Leadership and potential member candidates for a new identity utility dedicated for business participation and use.

## Proposal

Leverage the Sovrin Foundation as a fee-based provider of administration services for the management and delivery of a new DID Ledger under the did:sov root namespace. This new ledger, did:sov:bizid, will operate as a public utility provider under its own governance framework. A consortium of members will pay annual membership fees and provide supporting infrastructure to maintain a sustainable permissioned identity utility.

## Current Situation

Sovrin’s entry into the decentralized identity market began as a permissioned public ledger. Over the past three years, it has become an industry brand associated with decentralized identity. It represents more than an instance of a decentralized identity network based on a DLT, it is a trusted community of like-minded people and institutions from a variety of geographic regions and industry sectors. The Sovrin Community aspires to help all the entities (citizens, governments, businesses, devices) of the world to fix identity for both online and physical interactions.

During this same period, we have seen a global spotlight on privacy protection that has spawned regulation, such as GDPR and CCPA, which complements the spirit of the decentralized identity movement. However, these regulations also place additional financial risk and compliance constraints on businesses that desire to participate in and contribute to this privacy protection movement.

At the same time, the grassroots energy focused on “identity for all” has shifted or accelerated the thinking within the Sovrin Community towards a public permission-less utility that leverages a utility token. These philosophical changes, while socially acceptable, create a number of risk mitigation dilemmas for participating institutions. As a result, some businesses have exited the community while others have been hesitant to join.

To counter the pendulum bob swinging so far to the left, we have witnessed proposals for alternative proprietary solutions that reflect an unacceptable swing of the bob to the right. This oscillation between extremes depicts an opportunity to steer the pendulum bob to a center position that would allow institutions to strike a balance between open privacy by design and financial risks.

## Motivation

This proposal is intended to address three key concerns:

1. Policy Gridlock
2. Permissioned Safe Zone
3. Token-free Economics

### Policy Gridlock

The Sovrin approach for decentralized identity is to tackle it at global scale. The Sovrin Community, much like the global societies it seeks to represent, struggles with the formation of policies that can be embraced all at once by its members. The balancing of diversity goals at the operational level, risk mitigation for privacy regulation compliance, identity access for all, and the sustainability of a stable and reliable network is a non-trivial exercise. The technology adoption lifecycle teaches us that we cannot assume that all interested stakeholders will be able to embrace and adopt the technology at the same rate.

The Sovrin Foundation must find ways for it to [a] stay true to its vision; [b] aid all stakeholders on their decentralized identity journey; and [c] remain financially sustainable. Businesses and Governments around the world must be able to balance risk mitigation and technology adoption if Sovrin desires to be an open community for all. Additionally, all stakeholders must accept the fact that a single network (DID ledger) cannot serve the entire globe. As an example, the Sovrin Network uses Hyperledger Indy, which like many consensus algorithms, carries an expected threshold of optimal validator nodes, thereby limiting the scalability of a single network.

The decentralized identity community cannot afford to have disputes at the network level. We should be focused on market creation not market bifurcation. We live in a heterogeneous world of networks where interoperability is paramount. A single network cannot meet the needs of everyone and continued attempts to do so will minimally yield increased complexity and confusion. In fact, we have seen this within the Sovrin Foundation as it has been difficult to obtain closure after nearly a year on Version 2 of the Sovrin Governance Framework.

The fact is that the Sovrin Foundation has been in gridlock due to apprehension between policy decisions that may be necessary for one market segment and uncomfortable for another. This concern impacts the business market segment as well as external coalitions such as FINDY and KIVA who may desire to have their own governance framework while participating in the Sovrin Community. One approach to breaking the gridlock while still enabling two market segments to co-exist is to establish a community bound to a common vision but comprised of safe-spaces for each segment to establish their own governance.

### Permissioned Safe Zone

Preventive measures for avoiding the possible insertion of personal data into an immutable ledger has been the focus of much discussion. While many have agreed that a 100% guarantee is not possible, the implementation of a public write model only increases such exposure thereby making interested stakeholders more apprehensive to embrace a permission-less governance model. A diligent effort has been made within the Sovrin Foundation to address the GDPR risks associated community stakeholders. In collaboration with legal experts, the community has established a series of contractual instruments that address these risks for each stakeholder under both the public-write and permissioned write models. Unfortunately, this effort has resulted in a greater degree of complexity to the governance framework. It has also yielded an increase in costs for Stewards that need to comply with a broader set of technical and operational requirements.

One approach to reducing the complexity of governance policies is to transition the existing Sovrin Network (DID Ledger) into a dedicated ledger for public write access and then add a new DID Ledger that would operate under a separate governance model for permissioned writes.

### Token-free Economics

Sovrin is amidst a transition from the Sovrin Provisional Trust Framework to a new Sovrin Governance Framework that favors the use of a crypto-token to enable a payment model for public-write interactions with the ledger. The combination of public write access coupled with the conveniences of a payment token would open identity access up to a very diverse community that is currently unable to establish a trusted identity reputation.

While the social benefits of such an approach are appealing to many, the ability for many enterprises and some governments to embrace tokens at this point in time is limiting. Once again, a compromise that will allow two market segments to co-exist is to establish a community bound to a common vision but comprised of safe-spaces for each segment to establish their own governance.

## Common Ground

The pathway to a common vision for decentralized identity is rooted in open standards and open source communities. Both market segments of the Sovrin Community can agree on an *Open by Design* approach. While the members within each market segment may require incompatible governance models, both segments adamantly disagree with any deviation from an open approach at the technology or governance levels. Fundamentally, no single organization can own a network (system of ledgers) and the network must be built upon open standards and protocols where interoperability has been achieved.

Concepts

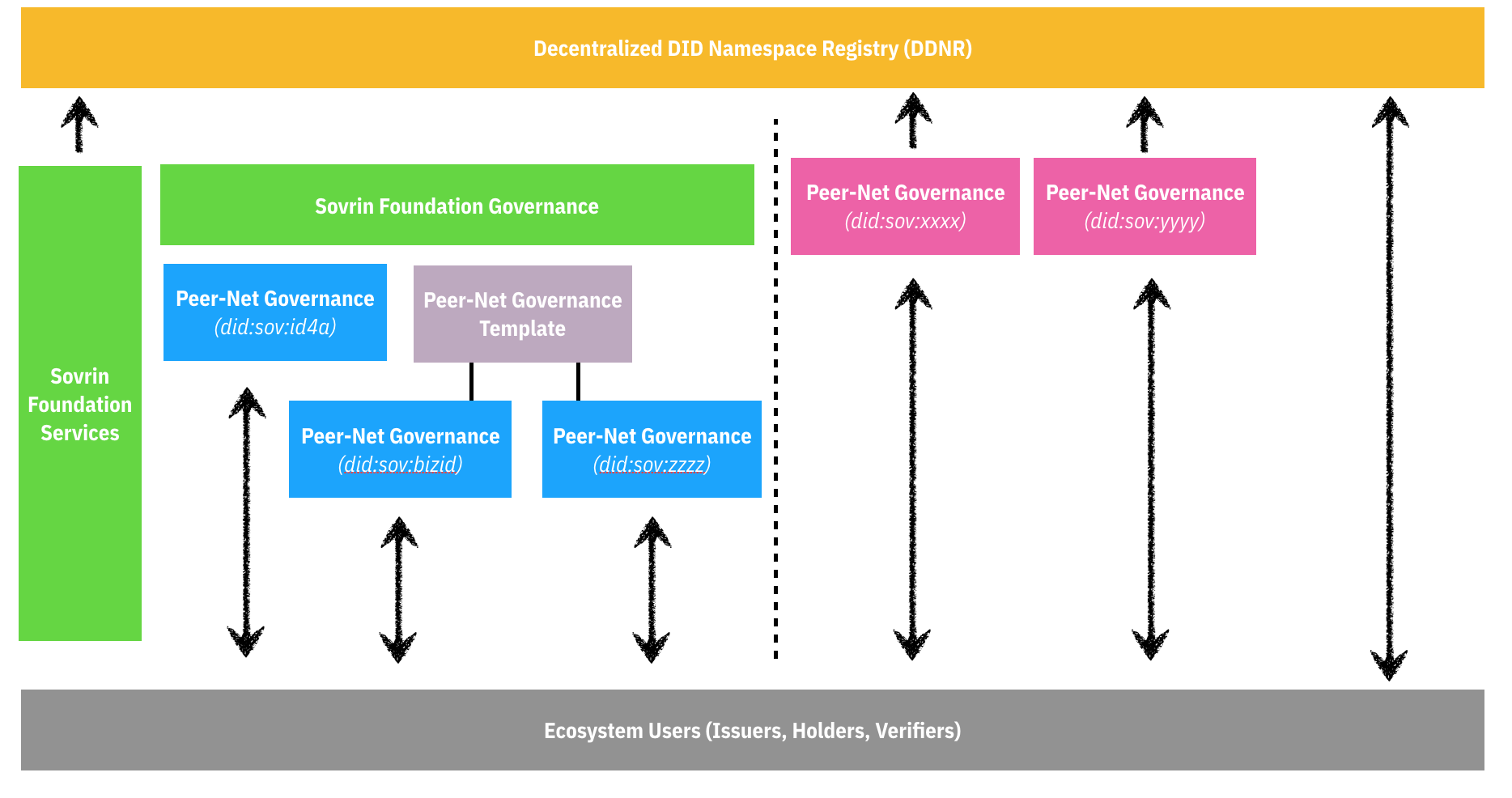


Figure : Network of Networks

* DID Namespace: Building on URI Standards, the DID Specification allows for both root namespace (did:xxx) and sub-namespace (did:xxx:yyy) conventions.
* Peer-Net: A distinct system of domain specific ledgers operated by decentralized peer nodes and associated with a DID Namespace.
* Network of Networks: A decentralized collection of discoverable and interoperable Peer-Nets. Each Peer-Net adheres to its own governance framework and the optimization limitations of the deployed DLT for consensus performance. The internet is already an exemplar of a network of networks structure based on DNS and URI standards.
* Decentralized DID Namespace Registry (DDNR): The DID Specification is already rooted in URI concepts, but it does lack a mechanism to address a decentralized approach to navigating a network of peer networks. A DDNR provides registration, discovery and validation of trusted Peer-Nets.
* Identity Utility Network: A Peer-Net governed by a consortium and preferably built on Hyperledger Indy.
* Identity Utility Administrator: The provider of operational and maintenance services for an Identity Utility Network. Such services may include:
  + Method Name registration services
  + Peer-Net activation services
  + DID Method resolution services
  + Namespace Registry Services
  + Trust Factor Certification Services
  + Build and Test Services
  + Consortium Coordination Services

## Approach

There are two potential solutions to the concerns raised herein: (1) establish a new Identity Utility Network and associated it with a new DID Root Namespace (did:bizid); or (2) establish a new Identity Utility Network and associated it with a new DID Namespace under the did:sov root namespace. While both are feasible, **Option 2** is preferred.

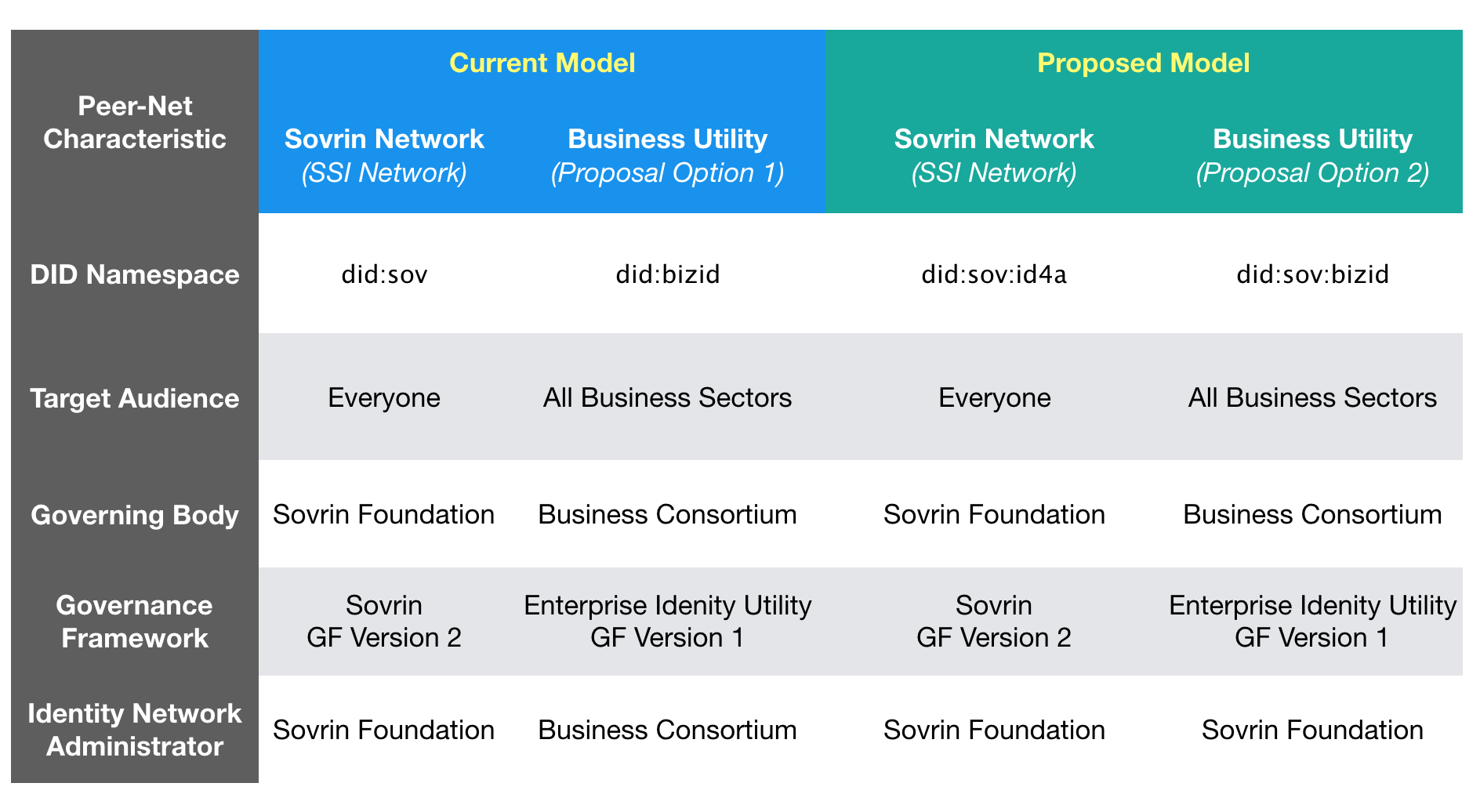


Table : Proposal Options

### Option 1: New DID Root Namespace

Collaborate with consortium of members that will deploy a Identity Utility Network (did:bizid) and define an enterprise grade governance framework which:

1. Enforces Permissioned Writes
2. Avoids Tokens
3. Establishes a governing board so no single organization owns the network
4. Requires adherences to a specific stack of open standards and protocols

Such an endeavor is a significant undertaking. It requires getting consortium agreement on a governance framework plus hiring staff to handle the operational and maintenance tasks for the Peer-Net. A benefit however is total autonomy.

### Option 2: Sovrin Namespace

Follow the same approach as Option 1 but leverage the Sovrin Foundation as an Identity Utility Administrator for the new Identity Utility Network (did:sov:bizid). This approach requires changes to the Sovrin Foundation and introduces a new financial sustainability model. The Sovrin Foundation already has skilled resources to tackle the operational and maintenance responsibilities for administrating a Peer-Net. These capabilities can be offered as fee-based services to the new consortium. To allow for this approach, the existing Sovrin Governance Framework would need to be refined (Version 3) to focus only on a public write token model and the current Identity Utility Network (did:sov) would need to be transitioned to did:sov:id4a (as an example).

## Governance Framework Concepts

### Common Concepts

| **Topic** | **Options 1 & 2** |
| --- | --- |
| Optimal Consensus Threshold | A balance between budget requirements and technology limitations will define the number of nodes required to operate the Identity Utility Network (“*Network*”). Initially this will be set at 13. The set of active nodes on the network will be periodically pulled from a pool of available nodes. |
| Membership  Types | 1. Founding Members    1. Limited to 15.    2. Members that are willing to contribute to the infrastructure, management, and financial needs of the *Network*.    3. Benefits       1. Seat on Board of Directors.       2. Automatic approval to operate as a Trust Anchor.       3. Unlimited transactions. 2. Stewards    1. Limited to 30.    2. Members that are willing to contribute to the infrastructure and financial needs of the *Network*.    3. Benefits       1. Automatic approval to operate as a Trust Anchor.       2. Unlimited transactions. 3. Trust Anchors: An unlimited number of members that are willing to be responsible for the endorsement of transactions to the ledger. They are obligated to use *Network* approved endorser software and accountable for vetting the entities performing write requests. |
| Board of Directors (BoD) | Founding Members will have the right to appoint a board director. Each Founding Member will be allocated one vote for each appointed Director. The BoD will establish a charter that will establish Officer roles and responsibilities. The BoD will establish terms for Officers, but no term shall exceed 3 years. |
| Budget | BoD is responsible for defining and approving the *Network* budget. Income for the budget will be derived from membership dues. The budget will be limited to expenses for the administration, operation, and maintenance of the *Network.* |
| Membership Dues | 1. Founding Members: $50K/yr 2. Stewards: $30K/yr 3. Trust Anchors    1. Enterprise Plan: 1000 write transactions/yr for $10K/yr    2. Service Provider Plan: 2500 write transactions/yr for $25K/yr |
| Membership Obligations | 1. Founding Members    1. Sign Steward Agreement    2. Sign Trust Anchor Agreement (*optional*)    3. Host 3 nodes (main, test, dev), each running *Network* approved code. 2. Stewards    1. Sign Steward Agreement    2. Sign Trust Anchor Agreement (*optional*)    3. Host 3 nodes (main, test, dev), each running *Network* approved code. 3. Trust Anchors    1. Sign Trust Anchor Agreement |

### Option Specific Concepts

| **Topic** | **Option 1** | **Option 2** |
| --- | --- | --- |
| Governance Framework | Refer to *Attachment A* as a template for building a new set of control and legal documents. | BoD will refine and prune the [SGFv2](https://sovrin.org/library/sovrin-governance-framework/) to create an acceptable set of control and legal documents for the *Network*. Refer to *Attachment A* for guidance. |
| Management | The BoD will be required to manage a budget and hire resources to staff the “day to day” management of the *Network*. These activities would include:   1. Financial Accounting 2. Legal 3. Public Communications 4. Technical Strategy & Architecture 5. Administrative 6. Build and Test 7. Membership Management | The BoD will be required to manage a budget and hire resources to coordinate the management of the *Network* using Sovrin Foundation as an Identity Utility Administrator.  The BoD will hire a *Network Manager* who will report to the BoD and will be responsible for activities such as:   1. Financial Accounting 2. Legal 3. Public Communications 4. Administrative 5. Membership Management   The BoD will appoint a representative of the *Network* to serve on the Sovrin Board of Trustees.  The BoD will hire a *Network Architect* whowill be responsible for interfacing with the Sovrin Foundation for activities such as:   1. Technical Strategy & Architecture 2. Build and Test |

## Inhibitors to Success

1. Sovrin Foundation Support *(only pertinent to Option 2)*.
2. Minimum Viable Consortium (nn Founding Members) needed to cover O&M expenses.
3. Open source implementation for DDNR.

# Attachment A: Governance Framework

Given the degree of work performed to date within the Sovrin Foundation in support of two market segments, the *creation of a new governance framework* primarily focused on just one of the market segments should begin with the pruning and refining of templates from Version 2 of the Sovrin Governance Framework.

|  |  |
| --- | --- |
| **Template** | **Suggested Action** |
| Sovrin Governance Framework Master Document | *Review and update scope, core principles, and core policies.* |
| Sovrin Glossary | *Work with Sovrin to separate terms from Appendices.* |
| Sovrin Trust Assurance Framework | *Review conformance of actors to polices.* |
| Sovrin Steward Agreement | *Review and update contractual instrument.* |
| Transaction Author Agreement | *Evaluate necessity/applicability. Review/Update if required.* |
| Transaction Endorser Agreement | *Review and update contractual instrument for use with Trust Anchors.* |
| Sovrin Governing Body Policies | *Review and update control document. Propose suggestions to Sovrin Foundation.* |
| Sovrin Ledger Access Policies | *Review and update control document.* |
| Sovrin Steward Business Policies | *Review and update control document.* |
| Sovrin Steward Technical Policies | *Review and update control document.* |
| Sovrin Economic Policies | *Not required.* |
| Sovrin Trust Mark Policies | *Review for consideration.* |
| Sovrin Steward Data Processing Addendum (DPA) | *Required. Review and update contractual instrument.* |
| Sovrin Steward Technical and Organizational Measures (TOMs) | *Required. Review and update contractual instrument. Consolidate with Steward Technical Policies.* |
| Sovrin Transaction Endorser DPA | *Required. Review and update contractual instrument.* |
| Sovrin Transaction Endorser TOMs | *Required. Review and update contractual instrument.* |