

DIGITAL GOVERNANCE INSTITUTE



POWERING THE ENGINE OF INTERNET TRUST

THE DIGITAL GOVERNANCE GUIDE

*CREATING TRANSPARENCY AND ACCOUNTABILITY
OVER DIGITAL TECHNOLOGY*

SCOTT S. PERRY, CPA, CISA
DIGITAL GOVERNANCE INSTITUTE



TABLE OF CONTENTS

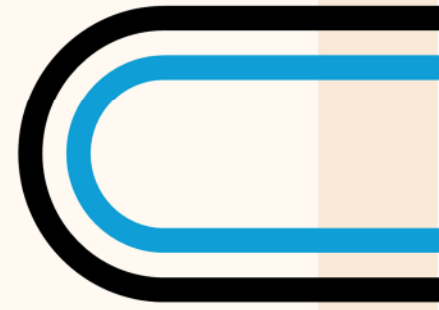
INTRODUCTION	3
EXECUTIVE SUMMARY	4
THE NEED FOR DIGITAL GOVERNANCE	5
MODEL FOR DIGITAL GOVERNANCE	8
GOVERNANCE CONSULTING	14

INTRODUCTION

Over the last 25 years, companies have continued to exploit the ubiquitous reach of the Internet despite the collateral damage caused by criminal opportunists and human error. Since the Internet is not centrally governed by one governing party, it becomes imperative on technology governance leaders to establish and oversee transparent requirements to hold participants in their domain accountable for the benefit of our digital society.

This distribution of control introduces new leaders to concept of digital governance. This Guide is intended to educate all to the concept of digital governance by introducing a risk-based methodology intended to create transparent rules shared within a community of technology service providers that hold themselves accountable for the benefit of all who want their information trusted in the digital world. To complement this methodology, we introduce a suite of services offered by the Digital Governance Institute to tailor this methodology to the needs of each community.

EXECUTIVE SUMMARY



The introduction of new technology (e.g. AI, verifiable credentials, blockchain, etc.) offers great benefit to increase societal trust over the source and content of digital information. However, implementing this technology broadly among a disparate group of service introduces significant challenges, similar to new laws that affect a wide swath of a population. In the digital world, collective management over technology takes governance.

Governance is the cyclical creation and monitoring of requirements over technology based on risk and the ability of service providers to electively hold themselves accountable for these requirements.

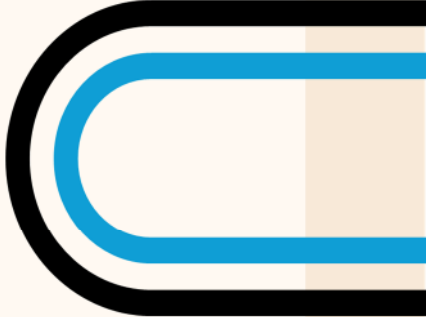
This Guide explores the need for digital governance based on our fragile trustworthiness of the Internet and the expanding drive to introduce high-value applications that rely upon the confidence users have over the source and content of digital information.

The Guide first introduces the following factors which have created an insecure medium for trusting sources and content on the Internet:

- 🏠 Anonymity and Pseudonymity
- 🏠 Ease of Content Creation and Sharing
- 🏠 Algorithm-Driven Content Distribution
- 🏠 Lack of Regulation
- 🏠 Echo Chambers and Filter Bubbles
- 🏠 Manipulation and Propaganda
- 🏠 Cybersecurity Threats
- 🏠 Rapid News Cycle, and
- 🏠 Global Reach and Cultural Differences.

Risk drives the need for trust. The Guide further summarizes the following risks that affect our confidence over the source and content of digital information:

- 🏠 Data Privacy Concerns
- 🏠 Cybersecurity Threats
- 🏠 Misinformation and Disinformation
- 🏠 Online Harassment and Hate Speech
- 🏠 Digital Divide
- 🏠 Emerging Technologies
- 🏠 Globalization of the Internet
- 🏠 Consumer Protection, and
- 🏠 Environmental Impact.



To address these risks, the Guide introduces a complete model for digital governance based on a toolkit authored for the Trust Over IP Foundation which incorporates a perpetual cycle of the following activities:

- 🏠 Risk Assessment
- 🏠 Governance Requirements
- 🏠 Conformance Program Development and Operation
- 🏠 Residual Risk Evaluation

The Guide also highlights critical success factors in deploying this methodology into successful digital governance frameworks.

Having a model and toolkit is often insufficient for governance implementations. To complement our toolkit and model, the Guide highlights the following consulting services offered by the Digital Governance Institute to assist governing authorities in establishing and operating governance frameworks and conformance programs:

- 🏠 Technology Risk Assessment
- 🏠 Establishing Conformance Roles
- 🏠 Determining Levels of Assurance
- 🏠 Governance Framework Creation
- 🏠 Identify Conformance Criteria
- 🏠 Trust Registry Governance Processes
- 🏠 Governance Assessment
- 🏠 Outsourced Governance Operation

Please read on to learn about digital governance in greater detail and contact us at the Digital Governance Institute at info@digitalgovernanceinstitute.com to open a dialogue about your specific needs or questions.

THE NEED FOR DIGITAL GOVERNANCE

Over the last 25 years, companies have continued to exploit the ubiquitous reach of the Internet despite the collateral damage caused by criminal opportunists and human error. The evolution of the Internet has created an insecure medium for trusting sources and content due to several interrelated factors:

- ❏ **Anonymity and Pseudonymity:** The ability for users to remain anonymous or use pseudonyms online makes it difficult to verify identities, leading to the spread of misinformation and deceptive practices.
- ❏ **Ease of Content Creation and Sharing:** With platforms allowing anyone to create and publish content, it has become challenging to distinguish between credible sources and unreliable ones. This democratization of information can lead to the proliferation of false or misleading content.
- ❏ **Algorithm-Driven Content Distribution:** Many social media platforms and news aggregators use algorithms that prioritize engagement over accuracy. This can amplify sensational or misleading content, making it more visible and trusted by users.
- ❏ **Lack of Regulation:** The relatively unregulated nature of the Internet allows for the spread of false information without accountability. Many platforms do not have stringent checks in place to verify the credibility of the sources or the content.
- ❏ **Echo Chambers and Filter Bubbles:** Users often curate their information sources, leading to echo chambers where they only receive information that reinforces their existing beliefs. This can distort perceptions of truth and reliability.
- ❏ **Manipulation and Propaganda:** The Internet has become a tool for deepfakes and opinion manipulation, with coordinated campaigns spreading disinformation for political, social, or financial gain. This challenges users' ability to discern trustworthy information.
- ❏ **Cybersecurity Threats:** The rise of cyber-attacks, including phishing and hacking, can compromise the integrity of information sources. Users may inadvertently trust compromised websites or content, leading to misinformation.
- ❏ **Rapid News Cycle:** The fast-paced nature of news dissemination online often prioritizes speed over accuracy. This can lead to the spread of unverified information before it can be fact-checked.
- ❏ **Global Reach and Cultural Differences:** Information can spread globally without cultural context, leading to misunderstandings and misinterpretations of content.

These factors contribute to an environment where users must be increasingly vigilant and skeptical about the sources and content they encounter online, often leading to confusion and mistrust. Society has passed the point-of-no-return of using a public network—but also no longer blindly trusts it. Demand for transparency and accountability of technology is growing. This Guide is for those leaders who want to

implement greater transparency and accountability in emerging technology so we can trust the source and content of digital information.

RISK DRIVES THE NEED FOR TRUST

This Guide would not exist if there were no threats to systems and networks operating as expected. In an Internet over 25 years old, we expect apps to function as designed, systems to be available when we need them, data to remain secure from prying eyes, and our private data to remain private. But these outcomes do not happen by themselves. They must be consciously built into our infrastructure by a cooperative array of information technology providers who design the controls necessary to address the following risks.

- 🏠 **Data Privacy Concerns:** With increasing awareness of data breaches and misuse of personal information, there is a growing demand for regulations that protect user privacy, such as the General Data Protection Regulation (GDPR) in Europe.
- 🏠 **Cybersecurity Threats:** The rise in cyber-attacks, including ransomware and phishing, necessitates governance frameworks to protect individuals and organizations from these threats.
- 🏠 **Misinformation and Disinformation:** The spread of false information, especially on social media platforms, has led to calls for regulations to ensure accountability and transparency in content moderation.
- 🏠 **Online Harassment and Hate Speech:** The prevalence of harassment and hate speech online has prompted demands for policies that protect users and create safer online environments.
- 🏠 **Digital Divide:** Disparities in access to the Internet highlight the need for governance to ensure equitable access to digital resources and opportunities, especially in underserved communities.
- 🏠 **Emerging Technologies:** Innovations like artificial intelligence, blockchain, and the Internet of Things (IoT) raise ethical and regulatory questions that require careful governance to mitigate risks.
- 🏠 **Globalization of the Internet:** As the Internet transcends borders, international cooperation and harmonization of laws are needed to address cross-border issues such as cybercrime and jurisdiction.
- 🏠 **Consumer Protection:** As online commerce grows, there is an increasing need for governance to protect consumers from fraud and ensure fair business practices.
- 🏠 **Environmental Impact:** The environmental footprint of digital technologies calls for governance to promote sustainable practices within the tech industry.

These factors collectively underscore the importance of establishing a governance framework of transparent rules and an accountability scheme to address the complexities of the modern Internet landscape.

MODEL FOR DIGITAL GOVERNANCE

The core to any governance framework is a recommended set of requirements that various players in the marketplace choose to adopt and implement to exact more trust over digital communications and data.

Prior to the establishment of governance framework over technology, an authoritative, “governing body” needs to identify the technology, and the disparate roles and actions that participate in the control of it and the level of confidence the body expects outside parties to rely on it.

The following diagram, defined by the Trust Over IP Foundation, introduces the relationship of a multi-layered set of technology driving the exchange of verifiable information located in secure smart wallets supported by underlying processes, service providers and infrastructure to a coordinated governance process that oversees the collective trust desired by the community:

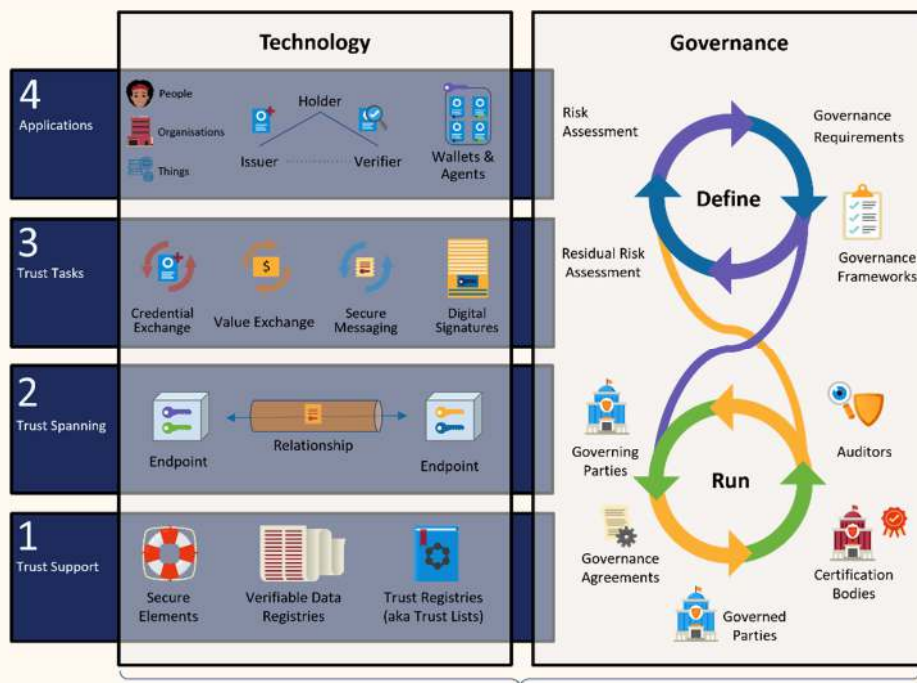


Figure 1: Relationship of Governance to a Multi-Layered Technology Stack

The decentralized nature of this participation requires a transparent and “opt-in” methodology to hold players collectively accountable to the governance program. This requires a governance methodology that is open, transparent, fair, and ultimately hold participants accountable for their conformance.

Let’s look further into the components of the governance processes in this model.



Figure 2: Digital Governance Model

RISK ASSESSMENT¹

A risk assessment is a subjective process to identify potential threats of and to the scope of technology that a governing body wants to collectively manage.

Risk assessments are used to identify, estimate, and prioritize risk factors that can negatively affect this scope of technology and the service provider's and even the governance body's ability to manage it. A comprehensive/systematic risk assessment needs to consider:

- ☑ **Relevant threats** to this scope including the artifacts and the roles entrusted to process them,
- ☑ **Vulnerabilities** within the scope and external threats related to our ability to rely on the source and content of information,
- ☑ **Impact** (i.e., harm) to governed parties that may occur given the potential for threats exploiting vulnerabilities, and
- ☑ **Likelihood** that this harm will occur.

The result is a determination of risk (typically a function of the qualitative impact of harm and its likelihood) and open decisions on how to treat the risk including using a cooperative governance framework to mitigate it.

GOVERNANCE REQUIREMENTS²

One of the risk treatment options of a risk assessment process is to mitigate risk or reduce it to an acceptable level. This can only be achieved if the governing authority can articulate the "governance requirements" or actions that community members must abide by to reduce risk.

¹ ToIP Risk Assessment Companion Guide (2021), The Trust Over IP Foundation

² ToIP Trust Assurance Companion Guide (2021), The Trust Over IP Foundation

- ❏ **Governing Authority** is an organization responsible for the conformance program. It can empower an Administering Party, charged with administering the Governing Party's Governance Framework, to manage the conformance program.
- ❏ **Governing Party** (either a Governing Authority itself or its proxy Administering Party) is an organization that defines 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. It recognizes Auditor Accreditors (and issues Audit Accreditor Credentials placing them on a Credential Registry) that set rules for the qualification of auditors and audits to hold governed parties accountable for these minimum standards for levels of assurance. It reviews participating party's performance audits and accredits them as meeting minimum standards for varying levels of assurance and issue credentials and may 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. It demonstrates compliance by listing the governed party in a trust registry and/or issuing 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 those criteria. They hold themselves out to a conformance scheme which evaluates their conformance posture 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 conformance 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 apply conformance criteria to the protection of Credentials in the Registry subject to audit. A Credential Registry is an optional component of the Ecosystem.

The effectiveness of a conformance program is contingent on its ability to hold governed parties accountable to its requirements and in reducing the risk to an acceptable residual level. Therefore, the conformance program assesses the design (at a point of time) of a governance framework's risk mitigation scheme and its operational effectiveness over time. Without it and other risk treatment

options, risk cannot be lowered below an inherent (untreated) risk impact score.

RESIDUAL RISK EVALUATION³

Risk treatments do not reduce risks to zero. Even the best risk governance programs do not prevent all risks from occurring. The assessment of risk remaining after applying a conformance scheme is known as residual risk.

Common residual risks will be realized through governed parties not complying with governance requirements. For example, a university ecosystem governance framework may mandate that all degree requirements must be thoroughly checked through a system of manual and automated controls to mitigate the risk of degree credentials being issued wrongly to individuals who have not satisfied degree requirements. This is dependent on the effectiveness of the manual and automated controls in place. Later, as a result of an annual audit, it was determined that those controls were not in place and operating effectively, resulting in a residual risk that a portion of degree credentials did not support valid satisfaction of degree requirements.

How much residual risk is acceptable? This is a valid question, and the answer is “it depends.” Residual risk can result in significant cost, loss of reputation, lack of confidence in the ecosystem and the governance framework to maintain an acceptable level of trust. It is up to the governing party and relying parties to determine the level of residual risk that is acceptable.

Bottom line, the effect of residual risk **MUST** be analyzed against the cost and effort of treatments needed to reduce it further in order to determine if those actions are justified. Residual risk should be deemed acceptable if the organization understands and accepts the risk given its risk tolerance. Risk mitigation steps should ensure that residual risk minimally meets that level. One component concerning the communication of risk assessment results is disclosure of likely residual risk. The process of disclosure effectively shares the residual risk with relying parties so they can appropriately gauge the level of trust they can expect from a governance framework to achieve the objectives defined within its disclosed scope.

CRITICAL SUCCESS FACTORS FOR DIGITAL GOVERNANCE

The value of a digital trust ecosystem is highly dependent on the integrity of the participating parties. Conflicts of interest must be identified and eliminated. Procedures driving compliance must be fair, open, clear, and timely. All Governed Parties need to feel that it is a strategic advantage to participate — not an obligation. Costs, both for certification fees and auditor engagements, must be reasonable and matched to the value they carry.

The trust criteria itself must have clear and cost-effective practices available to demonstrate compliance. The total compilation of compliance costs of all Governed Parties in aggregate must be less than the value individual Governed Parties perceive or commercially realize—or they will refuse to participate.

In our litigious society, Governed Parties are risk averse. It is critical that each Governed Party remains only accountable to the risk reasonably afforded to them. For example:

- 🏠 Governing (or Administering) Authorities must be accountable for the efficacy of conformance

³ ToIP Risk Assessment Companion Guide (2021), The Trust Over IP Foundation

criteria.

- 🏠 Governing (or Administering) Authorities must be accountable for their fair and open accreditation of Audit Accreditors and Actors.
- 🏠 Governed Parties must be accountable only for their asserted compliance to the conformance criteria for the role they are serving as defined in the relevant governance framework.
- 🏠 Auditors must be accountable for their attestation opinions.
- 🏠 Certification Bodies must be accountable for their certification of Governed Parties.
- 🏠 Audit Accreditors must be accountable for their accreditation of auditors.
- 🏠 Governing (or Administering) Authorities and Audit Accreditors must be accountable for the issuance of trust marks.

The model must be able to weed out non-conformance and apply right-sized penalties when challenged. Accreditation should not be easy but not overly onerous. Relying parties recognize when rubber-stamping is the norm. The accreditation process itself should be continuously monitored so it can evolve with changing technical advances and societal needs. Feedback loops should be established with inputs from all participants so continuous improvement is engineered into the model.

GOVERNANCE CONSULTING SERVICES

Governance over technology is complicated. Just as you would not endeavor to build a house solely on a blueprint, it should not be the same for technology governance. At the Digital Governance Institute, we complement our benchmark toolkit for digital governance and conformance operation with the following suite of consulting services designed to realize the objectives that governing authorities have over a set of technology:

TECHNOLOGY RISK ASSESSMENT:

We approach our risks assessments regardless of whether our clients have performed a risk assessment or not. If so, we'll first review their risk assessment and determine the gaps needed for its usage. The approach is to retrofit this information into an initial set of risks being addressed within the objectives of our clients, whether to develop conformant digital credentials or other risk-mitigating measures it intends to collaboratively control. Our methodology uses our toolkit, the [template provided by the Trust Over IP Foundation](#) using the risk assessment methodology and guidance provided by the [Risk Assessment Companion Guide](#).

After creating an initial set of risks, we hold dedicated sessions with our client's Governance Task Force to review the set of risks and solicit new ones. Next, we analyze the risks by likelihood and severity based on the use of these digital credentials and their acceptance outside the governance ecosystem. We then review the set of risk ratings with the Task Force. Then we triage the risks which are worthy of attaching risk mitigation measures and those deemed not worthy of the effort. We review this triage with the Task Force.

Next, we identify risk treatment options for the risks in scope. Those selected for risk treatment options will drive the development of conformance criteria. We review this risk treatment with the Task Force. Finally, we document "residual" risk, risk that cannot be addressed within the conformance program. This risk is considered the difference between "reasonable risk (at varying levels of assurance) and absolute risk mitigation (deemed too costly and time-consuming to be effectively treated).

The result of the Risk Assessment will be a Risk Assessment Matrix spreadsheet that will drive the rest of the conformance program.

ESTABLISHING CONFORMANT ROLES:

We analyze the various roles in the ecosystem and lead a discussion on plans and timing to hold each role accountable (or not). We seek concurrence during a session of the Governance Task Force.

The result of role assessment is a defined set of roles that will be included in the Governance Framework and Conformance Program and justification and alternative actions for roles not included in this scope.

DETERMINING LEVELS OF ASSURANCE:

We analyze various considerations of levels of assurance in the marketplace and within generally accepted schemes (e.g. GDPR, eIDAS 2.0, NIST 800-63, etc.) and present a recommended set of levels of assurance that will tier degrees of confidence that relying parties may take in the reliance of technology. We then lead a discussion with the Governance Task Force seeking concurrence.

The result of the levels of assurance determination is a defined set of confidence tiers that will be included in the Conformance Program.

GOVERNANCE FRAMEWORK CREATION:

Governance requirements are derived to mitigate risks selected during the risk assessment. A Governance Framework is developed that creates a transparent architecture description of all the components and information needed to convey to all ecosystem participants and relying parties how, why, and what they can rely upon for the use of the technology. The approach is to create a draft based on a [template created by the Trust Over IP Foundation](#) and its associated [Companion Guide](#).

This draft is reviewed by the Governance Task Force, and we hold facilitated sessions to build out and complete the framework.

IDENTIFY CONFORMANCE CRITERIA:

Conformance criteria is derived from MUST statements in the Governance Framework and allocated based on conformant roles and levels of assurance determined earlier in the program. The approach is to create a draft of conformance criteria using a trust criteria [template created by the Trust Over IP Foundation](#) and its associated [Companion Guide](#).

This draft is also reviewed by the Governance Task Force, and we plan facilitated sessions to build out and complete the criteria.

TRUST REGISTRY GOVERNANCE PROCESSES:

Best practices drive using a machine-readable list of approved roles that demonstrated satisfaction to a set of acceptance criteria. The following is a set of work activities that guide the Trust Registry governance process:

Trust Registry Application Form

With our experience with existing trust registry programs, we facilitate the development of a Trust Registry Application Form.

Trust Registry Governance Criteria

We look at other models for Trust Registry acceptance criteria and facilitate the Credential Trust Registry governance requirements with the Governance Task Force.

Trust Registry Application Evaluation and Acceptance Process:

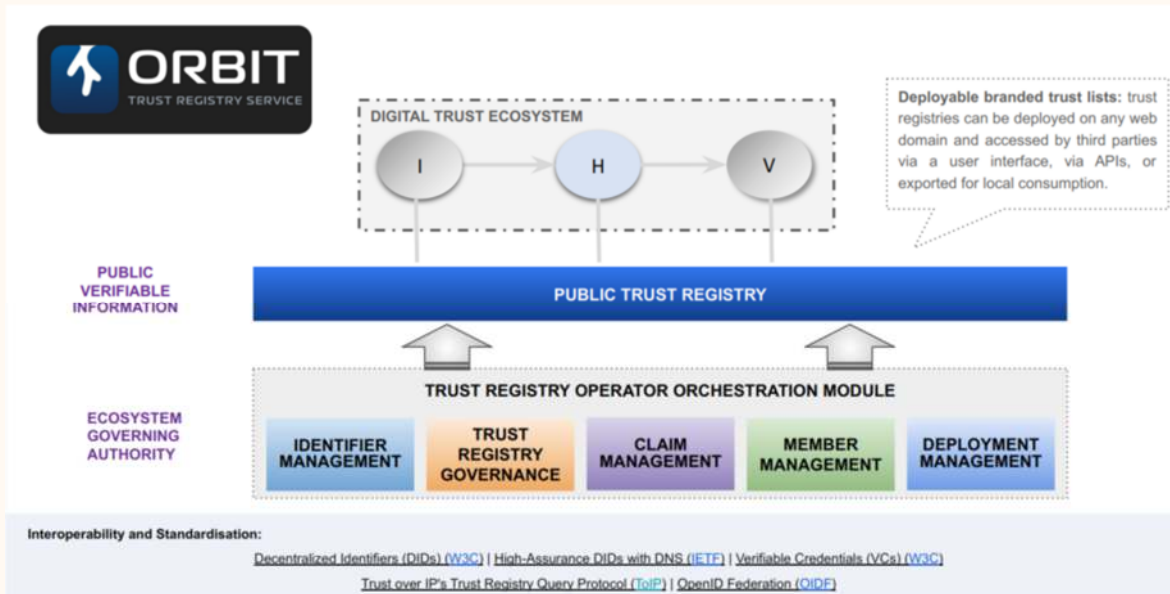
We draft a set of process steps and acceptance criteria that the Trust Registry program uses to evaluate and approve/reject applications and acceptance criteria from prospective registry applicants. It also contains processes for the removal of registry members from the trust registry.

Trust Registry Infrastructure Development and Implementation

The Digital Governance Institute has partnered with [Northern Block](#), a globally recognized provider of digital trust solutions (solutions (identity wallets, digital credential exchange toolkits, trust registries) to

develop and implement trust registries based on our governance methodology. Northern Block works with the client's technical team on the requirements, technical schedule, and costs of a robust trust registry infrastructure.

The following is the design of the Orbit Trust Registry Service Model:



GOVERNANCE ASSESSMENT

We assess our client's established digital governance framework and conformance program against our methodology identifying gaps and recommended actions to reduce risk, obtain greater market assurance and be more efficient in its operations.

OUSOURCED GOVERNANCE OPERATION

Our involvement with our clients does not stop after helping to establish a governance framework and/or conformance program. We can act as an Administering Authority, a proxy to our client's Governing Authority to execute its Governance Framework. The following services help operate our client's governance framework:

Accredit Third Party Auditors and Testing Laboratories

If our clients utilize third-party auditors and independent testing laboratories, we help them establish qualifications and acceptance criteria to enable these parties to participate in attesting to governance members conformance of their part in the Governance Framework. We review the qualifications and acceptance criteria with the Governance Task Force and issue Requests for Information (RFIs) and Requests for Proposal (RFPs) to solicit interest for the auditor and testing laboratory communities.

We objectively evaluate responses from these parties and make recommendations to the Governance Task Force for inclusion or denial of their participation in the governance ecosystem.

Review Third Party Audit and Testing Lab Attestation Reports

We objectively review conformance reports of ecosystem members from their third party audit firms and independent testing laboratories to determine continued satisfaction of governance requirements, if non-conformities are identified on these reports, we act as proxy to the governing body to address

remediation of these issues.

Residual Risk Evaluation

At least annually, we review trends in conformance reports of ecosystem members from their third party audit firms and independent testing laboratories to determine whether residual risk exists and whether additional governance requirements need to be established to mitigate those risks. We review our assessment with the Governance Task Force and use our Governance Framework methodology to affect needed amendments.

Governance Framework and Conformance Program Amendments

At least annually, together with the Residual Risk Evaluation described above, we facilitate a critical review of the Governance Framework and Conformance Program to determine what is working and what is not, whether market and technology considerations drive the need to amend governance and conformance program requirements. We execute this review by interviewing selected members of the ecosystem and ingest performance metrics of the governance operations.

We review our assessment with the Governance Task Force and use our Governance Framework methodology to affect needed amendments.

CALL TO ACTION

If you would like to learn more about how the Digital Governance Institute may help you to create a trustworthy community of technology through digital governance, please contact us at info@digitalgovernanceinstitute.com.

Scott Perry is the Founder and CEO of the Digital Governance Institute where he provides a variety of governance solutions in the emerging space of governance of digital assets. Scott is a recognized global leader in digital identity, blockchain, and verifiable credential governance and accreditation. He has worked with the world's most respected SSL-certificate issuers, aerospace and defense companies, and government agencies such as the US Senate Sergeant at Arms and Federal Aviation Administration.

He is a Co-Chair the Trust Over IP Foundation's Governance Stack Working Group where he has authored and contributed to most of its governance and assurance publications driven to create standards and accountability in decentralized identity and verifiable credential networks.

As a hands-on governance and cybersecurity consultant and auditor, Scott provides deep and impactful advice that you would expect from a leader in the field.