Identity and Verifiable Credential Risks

As part of an initial and ongoing governance process, Ecosystems must appropriately consider the risks affecting the set of transactions and credentials they are charged with governing. The attached matrix identifies risks related to digital identity and verifiable credentials at all layers of the ToIP stack:

Risk Assessment List						
RISK	**ToIP LAYER**	**TRUST AREAS AFFECTED**	**SEVERITY**	**LIKELIHOOD**	**RISK IMPACT**	**CONSIDERATIONS**
Governance Authority Risks						
Lack of competence to perform role	Ecosystem	Governance				Need for experienced personnel, proper training and governance framework
Lack of sufficient policy and practices	Ecosystem	Governance				Need for complete governance framework and feedback look
lack of consistency in operating practices of roles	Ecosystem	Governance				Requires proper oversight and trust assurance mechanisms
Lack of accountability of roles in network	Ecosystem	Governance				Requires proper oversight and trust assurance mechanisms
Lack of communication about governance practices	Ecosystem	Governance				Requires appropriate communication channels
Lack of appropriate authority	Ecosystem	Governance				Requires recognition and endorsement by relying parties
Ineffective bias in authority	Ecosystem	Governance				Requires even representation, voting standards and non-discrimination practices
Lack of Relying Party recognition	Ecosystem	Governance				Requires recognition and endorsement by relying parties
Ecosystem Lacks Jurisdictional Acceptance	Ecosystem	Governance				Requires Mapping of Jurisdictional Regulation
Ecosystem Lacks Industry Acceptance	Ecosystem	Governance				Requires Mapping of Industry Regulation
Ecosystem Issues Trust Marks Inappropriately or Without Basis	Ecosystem	Governance				Requires Adequate Trust Marks Policies
Ecosystem Allowing Inappropriate Actors to Participate in Network	Ecosystem	Governance				Requires Provider Evaluation and Acceptance Processes
Ecosystem Inappropriately Blacklisting or White Listing Other Ecosystems	Ecosystem	Governance				Requires Adequate Ecosystem Black and White Listing Processing
Issuer Risks						
Credential Issued without sufficient basis	Data Exchange	Data Integrity				Requires training, trust assurance practices and controlled practices
Credential Issued before appropriate proofing of basis	Data Exchange	Data Integrity				Requires training, trust assurance practices, controlled practices and proper workflow
Credential Issued in the wrong format or structure	Data Exchange	Data Integrity				Requires standard formats and formatting controls
Credential issued to impostors	Data Exchange	Security				Requires Trusted Issuers, trust assurance practices
Credential Lacking Uniqueness	Data Exchange	Data Integrity				Requires Appropriate Credential Serialization
Credential Becoming Obsolete	Data Exchange	Data Integrity				Requires Appropriate Credential Validity Periods
Lack of Credential Revocation	Data Exchange	Data Integrity				Requires Adequate Credential Status Checking Procedures
Identity Proofing Practices Inadequate for Level of Assurance	Data Exchange	Data Integrity				Requires Ecosystem Governance Conformance Procedures
Issuer Practices Not Accepted by Ecosystem	Ecosystem	Governance				Requires Issuer Practice Conformance Procedures
Issuer Operations Unavailable	Data Exchange	Availability				Requires Network Redundancy Procedures
Verifier Risks						
Lack of competence to perform role	Data Exchange	Governance				Requires training, trust assurance practices and controlled practices

Lack of consistent verification practices	Data Exchange	Data Integrity				Requires training, trust assurance practices and controlled practices
Missing verification	Data Exchange	Data Integrity				Requires training, trust assurance practices and controlled practices
Untimely verification	Data Exchange	Data Integrity				Requires time-based controls
Evidence of verification incomplete or in incorrect format	Data Exchange	Data Integrity				Requires standard formats and formatting controls
Verifier Practices Not Accepted by Ecosystem	Ecosystem	Governance				Requires Verifier Conformance Procedures
Suspended Credential Being Accepted	Data Exchange	Data Integrity				Requires Adequate Credential Suspension Processes
Revoked Credential Being Accepted	Data Exchange	Data Integrity				Requires Adequate Credential Status Checking Procedures
Man-In-The-Middle Attack During Legitimate Verification	Data Exchange	Security				Requires Verifier Vulnerability Practices
Verifier Network Unavailable	Data Exchange	Availability				Requires Network Redundancy Procedures
Credential Registry Risks						
Lack of competence to perform role	Data Exchange	Governance				Requires training, trust assurance practices and controlled practices
Unavailable registry	Data Exchange	Availability				Requires availability controls
Lack of appropriate access to registry	Data Exchange	Security				Requires appropriate access controls
Inappropriate access writes to registry	Data Exchange	Data Integrity				Requires appropriate access management controls
Breach of registry	Data Exchange	Security				Requires appropriate security perimeter, breach detection and notification controls
Exploited Use of Stolen Credentials	Data Exchange	Data Integrity				Requires Adequate Breach Notification Processes
Credential Registry Not Accepted by Ecosystem	Ecosystem	Governance				Requires Credential Verifier Conformance Procedures
Audit Accreditor Risks						
Insufficient vetting of auditor population	Ecosystem	Governance				Requires training, and generally accepted auditor accreditor practices
Lack of competence to perform role	Ecosystem	Governance				Requires training, and generally accepted auditor accreditor practices
Auditor Risks						
Lack of competence to perform role	Ecosystem	Governance				Requires training, sufficient experience and generally accepted auditor practices
Credential Holder Risks						
Holder Threat of Litigation over Issuer	Data Exchange	Confidentiality				Proper Agreement in pace between Issuer and Holder detailing rights.
Counterfeit Credentials Being Created	Data Exchange	Data Integrity				Requires Adequate Credential Non-Repudiation Practices
Lack of Binding Between Holder and Credential	Data Exchange	Data Integrity				Requires Adequate Wallet Protection Measures
Credential Holder Given Inappropriate Access Rights	Data Exchange	Security				Requires Adequate User Enrollment Processes
Imposter Using Valid Credential	Data Exchange	Security				Requires Adequate Wallet Protection Measures
Credential Wallet Private Key is Compromised	Data Exchange	Security				Requires Adequate User Wallet Protection Measures
Credential Holder's Private Data is Compromised	Data Exchange	Privacy				Requires Adequate User Wallet Protection Measures
Lack of Portability of Credential	Data Exchange	Data Integrity				Requires Adequate Credential Interoperability Practices
Lack of Credential Federation Across Ecosystems	Ecosystem	Governance				Requires Adequate Credential Interoperability Practices

Exploited Private PIN Code Capture	Data Exchange	Confidentiality				Requires Adequate Wallet Protection Measures
Social Engineering Attacks Successfully Gather Credentials by Perpetrators	Data Exchange	Security				Requires Adequate Wallet Protection Measures
Provider Risk						
Provider Software Does not Operate as Intended	Provider	Data Integrity				Requires Adequate Provider SDLC Processes
Provider Software Does Not Operate on User Devices	Provider	Data Integrity				Requires Adequate Provider SDLC Processes
Provider Code Updates Cause Operational Issues	Provider	Data Integrity				Requires Adequate Provider SDLC Processes
Provider System Unavailable	Provider	Availability				Requires Adequate Provider Hardware Integration Practices
Utility Risks						
Inconsistent Steward Acceptance Practices	Utility	Governance				Requires Adequate Utliity Steward Acceptance Practices
Stewards Not Abiding by Governance Practices	Utility	Governance				Requires Adequate Steward Conformance Practices
Stewardship Not Available to Qualified Applicants	Utility	Governance				Requires Adequate Utliity Steward Acceptance Practices
Utility Not a Viable Going Concern	Utility	Governance				Requires Adequate Utility Monitoring Practices
Utility Using an Ineffective Consensus Model	Utility	Governance				Requires Adequate Utility Monitoring Practices
Utility Consensus Model Not Operating as Designed.	Utility	Governance				Requires Adequate Utility Monitoring Practices
Utility Charging Inaccurate Fees For Service	Utility	Governance				Requires Adequate Utility Monitoring Practices
Inadequate Number of Stewards for Consensus Protocol	Utility	Governance				Requires Adequate Utility Monitoring Practices
Inadequate Infrastructure Supporting Steward Operations	Utility	Availability				Requires Adequate Steward Conformance Practices
Inadequate Network Throughput Supporting Steward Operations	Utility	Availability				Requires Adequate Steward Conformance Practices
Inadequate Network Availability Supporting Steward Operations	Utility	Availability				Requires Adequate Steward Conformance Practices