verifiable LEI (vLEI) Ecosystem Governance Framework Risk Assessment

RISK No.	RISK	ToIP LAYER	TRUST AREAS AFFECTED	SEVERITY	LIKELIHOOD	RISK IMPACT	RISK CONSIDERATION ACTIONS	RISK TREATMENT	RISK TREATMENT ACTION	RESIDUAL RISK
	Governance Authority (GLEIF) Risks						GLEIF – Global Legal Entity Identifier Foundation operates and manages the Global LEI System (GLEIS);			
	Lack of competence to perform role	Ecosystem	Governance	4	1	LOW-MEDIUM	Need for experienced personnel, proper training and governance framework	Mitigation	Mitigated by proper, regular training	Residual risk regarded to be low and acceptable.
	Lack of sufficient policy and practices	Ecosystem	Governance	1	1	LOW	Need for complete governance framework and feedback loop	Mitigation	Mitigated by GLEIF supplied vLEI Issuer software	Residual risk regarded to be low and acceptable.
	Lack of consistency in its own operating practices	Ecosystem	Governance	3	1	LOW	Requires independent oversight and trust assurance mechanisms	Acceptance	Covered by ISO 20000 certification along with systematic control	Residual risk regarded to be low and acceptable.
	Lack of consistency in operating practices of vLEI Issuers	Ecosystem	Governance	3	3	MEDIUM	Requires proper oversight and trust assurance mechanisms	Mitigation	Mitigated by Ecosystem Governance Framework, vLEI Issuer Credential Qualification Program and use of KERI	Residual risk regarded to be low and acceptable.
	Lack of accountability of roles in network	Ecosystem	Governance	3	1	LOW	Requires proper supervisory and legal oversight and trust assurance mechanisms	Mitigation	Mitgated by Ecosystem Governance Framework, and specifically for vLEI Issuers, the Credential Qualification Agreement	Residual risk regarded to be low and acceptable.
	Lack of legal enforcability of Verifiable Credentials (VCs) in jurisdictions	Ecosystem	Governance	5	3	MEDIUM-HIGH	Requires monitoring of VC legal acceptance	Mitigation	GLEIF is researching and monitoring the legal enforcability of VCs in jurisdictions.	Residual risk regarded to be low and acceptable.
	Ecosystem Lacks Industry Acceptance or insufficient demand	Ecosystem	Governance	4	3	MEDIUM	Requires members of ecosystems to agree to use the vLEI	Mitigation	Work with industries to support their use cases with vLEI for organizational identification needs	Residual risk regarded to be low and acceptable.
	Qualified vLEI Issuer Risks						Qualified vLEI Issuer – An organization qualified by GLEIF to issue Legal Entity vLEI Credentials and to issue vLegal Entity Official Organizational Role vLEI Credentials			
	vLEI Legal Entity Credential or vLEI Legal Entity Official Organizational Role Credential issued without appropriate verification	Credential	Processing Integrity	5	3	MEDIUM-HIGH	Requires training, trust assurance practices, controlled practices and proper workflow	Mitigation	Require validation of the Legal Entity's Authorized vLEI Representatives (AVRs), Legal Name and Title of OOR Credential Holder, verification of control of KERI DID. Include a Verifier/Approver workflow in vLEI Issuer operations	Residual risk regarded to be low and acceptable.
	Credential Lacking Uniqueness	Credential	Processing Integrity	5	3	MEDIUM-HIGH	Requires Appropriate Check for Credential Duplication	Mitigation	Include a check to prevent duplicate vLEI Legal Entity Credentials and LEI Legal Entity Official Organizational Role Credentials	Residual risk regarded to be low and acceptable.
	vLEI Legal Entity Credential Becoming Invalid	Credential	Security	5	3	MEDIUM-HIGH	Requires Appropriate Monitoring of obligations of Legal Entities holding vLEIs	Mitigation	Monitoring of the status of the Legal Entity's LEI	Residual risk regarded to be low and acceptable.
	vLEI Legal Entity Official Organizational Role Credentials Becoming Invalid	Credential	Security	1	1	LOW	Requires Appropriate Action by Legal Entities to manage their Role Credentials	Acceptance	Risk is not to GLEIF. Legal Entities will be solely responsible for the management of issued Role Credentials and the composition of their organizational wallets.	Residual risk regarded to be low and acceptable.
	vLEI Issuer Operations Unavailable	Credential	Availability	5	3	MEDIUM-HIGH	Requires Network Redundancy Procedures	Mitigation	Require contingency and systen redundancy	Residual risk regarded to be low and acceptable.
	vLEI Issuer using obsolete and/or untested GLEIF supplied vLEI Issuer software or APIs	Credential	Processing Integrity	5	3	MEDIUM-HIGH	Requires change management process for vLEI Issuers	Mitigation	Change management process included in Credential Qualification Agreement. GLEIF to manage the change management process for vLEI Issuers	Residual risk regarded to be low and acceptable.
	Verifier Risks						Verifier - An entity that is verifying the components and provenance of a vLEI credential for a use case			
	Lack of consistent verification practices	Credential	Security	4	1	LOW-MEDIUM	Requires training, trust assurance practices and controlled practices	Mitigation	Mitigated by educating Verifiers of the existence of proof requests to verify credentials	Residual risk regarded to be low and acceptable.
	Evidence of verification incomplete or in incorrect format of proof requests	Credential	Processing Integrity	5	2	MEDIUM	Requires standard formats and formatting controls for proof requests	Mitigation	Develop standard formats and formatting controls for proof requests	Residual risk regarded to be low and acceptable.
	Revoked Credential Being Accepted.	Credential	Security	5	2	MEDIUM	Requires Adequate Credential Status Checking Procedures	Mitigation	KERI will prevent the use of revoked credentials.	Residual risk will be the time between request to revoke is made by the Legal Entity and actual revocation at the Qualified vLEI Issuer.
	Man-In-The_middle Attack During Legitimate Verification	Credential	Security	5	3	MEDIUM-HIGH	Requires Verifier Vulnerability Practices	Mitigation	Mitigate with security in GLEIF supplied vLEI Issuer software	Residual risk regarded to be low and acceptable.
	Verifier Network Unavailable	Credential	Availability	5	3	MEDIUM-HIGH	Requires Network Redundancy Procedures	Mitigation	Mitigate with appropriate system redundancy and contingency	Residual risk regarded to be low and acceptable.
	GLEIF Credential Registry Risks					LOW	GLEIF manages its own Credential Registry. These are risks associated with that repository.			
	Lack of competence to perform role	Credential	Governance	5	1	LOW-MEDIUM	Requires training, trust assurance practices and controlled practices	Mitigation	Mitigated by proper, regular training	Residual risk regarded to be low and acceptable.
	Unavailable registry	Credential	Availability	5	3	MEDIUM-HIGH	Requires availability controls	Mitigation	Mitigate with appropriate system redundancy and contingency	Residual risk regarded to be low and acceptable.
	Lack of appropriate access to registry	Credential	Security	5	3	MEDIUM-HIGH	Requires appropriate access controls	Mitigation	Mitigate with effective access controls	Residual risk regarded to be low and acceptable.
	Inappropriate access writes to registry	Credential	Security	5	2	MEDIUM	Requires appropriate access management controls	Mitigation	Mitigate with security in GLEIF supplied vLEI Issuer software	Residual risk regarded to be low and acceptable.
	Breach of registry	Credential	Security	5	2	MEDIUM	Requires appropriate security perimeter, breach detection and notification controls	Mitigation	Mitigate with security in GLEIF supplied vLEI Issuer software	Residual risk regarded to be low and acceptable.
	Exploited Use of Stolen Credentials.	Credential	Security	5	2	MEDIUM	Requires Adequate Breach Notification Processes			Residual risk regarded to be low and acceptable.
	GLEIF vLEI Issuer Qualification Program Risks						GLEIF operates its own Qualification program. These are the risks associated with that program.			
	Lack of competence to perform role	Ecosystem	Governance	1	1	LOW	Requires training, sufficient experience and generally accepted auditor practices	Mitigation	Mitigated by proper, regular training	Residual risk regarded to be low and acceptable.
	Inconsistent or biased qualification process	Ecosystem	Governance	2	1	LOW	Requires well-documented requirements and process, applied consistently	Mitigation	Mitigated by comprehensive program, applied consistently	Residual risk regarded to be low and acceptable.
	Legal Entity Risks						Legal Entity – a legal person or structure that is organized under the laws of any jurisdiction that meets the eligibility criteria for registering for a LEI.			
	Counterfeit Credentials Being Created.	Credential	Privacy	5	1	LOW-MEDIUM	Requires Adequate Credential Non-Repudiation Practices	Mitigation	Mitigated, since an invalid LEI would never appear and could not be checked in the GLEIS and a counterfeit vLEI never would be able to connect to the chain of trust of the vLEI system.	Residual risk regarded to be low and acceptable.
	Lack of Binding Between Legal Entity and Credential.	Credential	Confidentiality	5	2	MEDIUM	Requires Adequate Role Credential Issuance Measures	Mitigation	This risk must be tackled at the issuance stage. FIrst, the vLEI Issuer will verify that the Holder is in control of their DID. OOR Credentials will have role lists that can act as a guide for the types of OORs expected for the entity legal form of the Legal Enity, preventing OOR Credential issuance for bogus official roles. Assigning roles for Engagement Context Role Credentials entirely will be the responsibiity of the Legal Entity. The QVI will be responsible for Identity Verification.	Residual risk regarded to be low and acceptable.
	Imposter Using Valid vLEI Legal Entity Credential.	Credential	Security	5	2	MEDIUM	Requires Adequate Wallet Protection Measures	Mitigation	There will be a list of requirements/features for wallets holding credentials and that will be relied upon by Credential Holders.	Residual risk is that Holders do not adequately protect their wallets and prevent coersion despite the guidance and requirements in the vLEI Ecosystem Governance Framework.
	Credential Wallet Private Key or PIN is Compromised	Credential	Security	5	5	HIGH	Requires Adequate Protection Measures for Private Keys and PINs	Mitigation	Mitigated by KERI prerotation and effective wallet management. The best mitigation for a wallet's access key or PIN is to use multi-signatures for the identfier which means that multiple wallets must be compromised. Thus compromise of one wallet PIN or private key does not result in loss of control of the identifier.	Residual risk regarded to be low and acceptable.
	Lack of Portability of Credential	Credential	Availability	5	2	MEDIUM	Requires Adequate Credential Interoperability Practices	Mitigation	KERI will provide Credential portability.	Residual risk regarded to be low and acceptable.
	Lack of Credential Federation Across Ecosystems	Ecosystem	Availability	5	3	MEDIUM-HIGH	Requires Adequate Credential Interoperability Practices	Mitigation	The vLEI is designed as an Ecosystem Governance Framework to be able to interoperate within other ecosystems.	Residual risk regarded to be low and acceptable.
	Social Engineering Attacks Sucessfully Gather Credentials by Perpetrators	Credential	Security	5	2	MEDIUM	Requires Adequate Wallet Protection Measures	Mitigation	Credentials will be cryptographically bound to wallets and can be biometrically bound to Holders	Residual risk regarded to be low and acceptable.
	Utility Risks						Risks associated with KERI infrastructure (Part 1) and vLEI Credentials (Part 2)			
	GLEIF supplied software contains undetected bugs or defects that can be exploited by attackers. *	Utility	Security	5	2	MEDIUM	GLEIF supplied software should be tested and/or reviewed or audited for bugs and defects, internally and externally	Mitigation	All GLEIF supplied software will be publicly available open source code that will be conformance tested prior to distribution. A TVA (Topological Vulnerability Analysis) scan can be requested to be performed for new applications.	Residual risk regarded to be low and acceptable.
	Inadequate protection of pre-rotated sets of keys*	Utility	Security	5	1	LOW-MEDIUM	Training and monitoring of key management practices	Mitigation	Can be tested using a third-party security risk assessment against KERI Key Management Requirements	Residual risk regarded to be low and acceptable.
	Best practices for code delivery and library usage not followed for signature verification infrastructure*	Utility	Security	5	1	LOW-MEDIUM	Training and monitoring of best practices implemented	Mitigation	Can be tested using a third-party security risk assessment against KERI Key Management Requirements	Residual risk regarded to be low and acceptable.
	The specific holders of cryptographic keys have not been kept confidential.*	Utility	Security	3	2	LOW-MEDIUM	Training and monitoring of key management practices	Mitigation	Can be tested using a third-party security risk assessment against KERI Key Management Requirements	Residual risk regarded to be low and acceptable.
	The time and place of key rotation have not been kept confidential among the key holders until after the rotation has been completed.*	Utility	Security	3	2	LOW-MEDIUM	Training and monitoring of key management practices	Mitigation	Can be tested using a third-party security risk assessment against KERI Key Management Requirements	Residual risk regarded to be low and acceptable.
	Qualified vLEI Issuers have not monitored their public Verifiable Data Registry (VDR) for vLEI issuance and revocation registry for erroneous or malicious issuances and revocations.	Utility	Security	5	1	LOW-MEDIUM	Secondary monitoring by GLEIF	Mitigation	GLEIF secondary Witness monitoring program	Residual risk regarded to be low and acceptable.

**Note: Utility layer risks also can affect the higher layers.*

LEGEND		
COLUMN HEADER	EXPLANATION	Potential Values
Risk #	A unique identifier of a risk for reference purposes	#
Risk Description	Description of a unique risk	Text
ToIP Layer	The Governance Stack Layer the risk operates based on the ToIP Governance Stack	Ecosystem Credential Provider Utility
Trust Area Affected	Information trust component affected by the risk	Governance Availability Security Availability Privacy Processing Integrity
Severity	Judgmental evaluation of impact the risk would have on the entity if realized	Negligible Minor Moderate Major Critical
Liklihood	Judgmental evaluation of the potential that the risk will occur risk without controls or other circumstances to prevent it.	Highly Unlikely Unlikely Possible Likely Highly Unlikely
Impact	Judgmental scoring of risk's effect based on severity and and likelihood.	Low Low-Medium Medium Medium-High High
Risk Consideration Actions	Factors to consider regarding risk treatment	Text
Risk Treatment	Recommended action category to take to handle the risk	Mitigation Avoidance Transference Acceptance Other
Risk Treatment Action	High level action identified to treat risk	Text
Residual Risk	Judgmental level or state of risk after applying risk treatment	Text or Impact Level

SCALE OF LIKELIHOOD		NEGLIGIBLE (1)	MINOR (2)	MODERATE (3)	MAJOR (4)	CRITICAL (5)
	HIGHLY UNLIKELY (1)	LOW	LOW	LOW	LOW - MEDIUM	LOW - MEDIUM
	UNLIKELY (1)	LOW	LOW - MEDIUM	LOW - MEDIUM	MEDIUM	MEDIUM
	POSSIBLE (3)	LOW	LOW - MEDIUM	MEDIUM	MEDIUM	MEDIUM-HIGH
	LIKELY (4)	LOW - MEDIUM	MEDIUM	MEDIUM	MEDIUM-HIGH	HIGH
	HIGHLY LIKELY (5)	LOW - MEDIUM	MEDIUM	MEDIUM-HIGH	HIGH	HIGH