**Version Date:** 2022-12-16

**Status: Final**

DID URL for Risk Assessment:
did:keri:EINmHd5g7iV-UldkkkKyBIH052bIyxZNBn9pq-zNrYoS?service=vlei-documents&relativeRef=/egf/docs/2022-12-16_verifiable-LEI-(vLEI)-Ecosystem-Governance-Framework-Risk-Assessment_v1.0_final.xlsx

# verifiable LEI (vLEI) Ecosystem Governance Framework 1.0 Risk Assessment — Document Version 1.0 — 2022-12-16

| RISK No. | RISK | TOIP Layer | TRUST AREAS AFFECTED | SEVERITY | LIKELIHOOD | RISK IMPACT | RISK CONSIDERATION ACTIONS | RISK TREATMENT | RISK TREATMENT ACTION | RISIDUAL RISK |
|---|---|---|---|---|---|---|---|---|---|---|
| | **GOVERNING 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 workflows supported by KERI vLEI 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 Qualified vLEI Issuers | Ecosystem | Governance | 3 | 3 | MEDIUM | Requires proper oversight and trust assurance mechanisms | Mitigation | Mitigated by Ecosystem Governance Framework, vLEI Issuer Qualification Program and use of Key Event Receipt Infrastructure (KERI) protocol | 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 Qualified vLEI Issuers, the vLEI Issuer Qualification Agreement | Residual risk regarded to be low and acceptable. |
| | Lack of legal enforcability of Authentic Chained Data Container (ACDC) credentials in jurisdictions | Ecosystem | Governance | 5 | 3 | MEDIUM-HIGH | Requires monitoring of ACDC legal acceptance | Mitigation | GLEIF is researching and monitoring the legal enforcability of ACDCs 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 Legal 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 | Requires authorization by Legal Entity's Authorized Representatives (LARs), Identificaton of the person and Official Organizational Role (OOR) of the OOR Person, verification of control of KERI DID. Include a Issuer/Approver workflow in Qualified vLEI Issuer operations | Residual risk regarded to be low and acceptable. |
| | Legal Entity vLEI 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 by Qualified vLEI Issuers | Residual risk regarded to be low and acceptable. |
| | Legal Entity Official Organizational Role vLEI Credentials becoming invalid | Credential | Security | 1 | 1 | LOW | Requires appropriate action by Legal Entities to manage their vLEI Role Credentials | Acceptance | Risk is not to GLEIF. Legal Entities will be solely responsible for the management of vLEI Role Credentials issued and the composition of their organizational wallets. | Residual risk regarded to be low and acceptable. |
| | Qualified vLEI Issuer operations unavailable | Credential | Availability | 5 | 3 | MEDIUM-HIGH | Requires network redundancy procedures | Mitigation | Requires contingency and systen redundancy | Residual risk regarded to be low and acceptable. |
| | Qualified vLEI Issuer using obsolete and/or untested vLEI software or APIs | Credential | Processing Integrity | 5 | 3 | MEDIUM-HIGH | Requires change management process for Qualified vLEI Issuers | Mitigation | Change management process included in the vLEI Issuer Qualification Agreement. GLEIF to manage the change management process for Qualified 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 vLEI being accepted | Credential | Security | 5 | 2 | MEDIUM | Requires adequate vLEI status and validity checking procedures | Mitigation | Mitigated by KERI vLEI software that automatically checksrevocation status before accepting a credential | 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 KERI vLEI 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** | | | | | | 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 KERI vLEI 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 KERI vLEI software | Residual risk regarded to be low and acceptable. |
| | Exploited use of stolen vLEIs | Credential | Security | 5 | 2 | MEDIUM | Requires adequate breach notification processes | Mitigation | Mitigated by use of KERI vLEI software with the vLEI Reporting API | Residual risk regarded to be low and acceptable. |
| | **GLEIF vLEI Issuer Qualification Program Risks** | | | | | | GLEIF operates its own vLEI Issuer 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 (not based on valid LEIs) being issued | 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 vLEIs issued | Credential | Confidentiality | 5 | 2 | MEDIUM | Requires adequate vLEI Role Credential issuance measures | Mitigation | This risk must be tackled at the issuance stage. First, the QVI only can issue on receipt of a QVI Authorization vLEI sent by the Legal Entity Authorized Representatives (LARs). Then,as part of the Identity Verification process, the QVI will verify that the OOR Person is in control of their DID. OOR vLEI Role 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. | Residual risk regarded to be low and acceptable. |
| | Imposter using valid Legal Entity vLEI 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 vLEI 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. |
| | Private signing key is compromised | Credential | Security | 5 | 5 | HIGH | Requires adequate protection measures for private keys | Mitigation | Mitigated by KERI prerotation and effective wallet management.<br>The best mitigation for a wallet's access key is to use multi-signatures for the identfier which means that multiple wallets must be compromised. Thus compromise of one wallet private key does not result in loss of control of the identifier. | Residual risk regarded to be low and acceptable. |
| | Lack of portability of vLEIs | Credential | Availability | 5 | 2 | MEDIUM | Requires adequate vLEI interoperability practices | Mitigation | KERI will provide vLEI 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. |

## verifiable LEI (vLEI) Ecosystem Governance Framework 1.0 Risk Assessment — Document Version 1.0 — 2022-12-16

| RISK No. | RISK | TOIP Layer | TRUST AREAS AFFECTED | SEVERITY | LIKELIHOOD | RISK IMPACT | RISK CONSIDERATION ACTIONS | RISK TREATMENT | RISK TREATMENT ACTION | RISIDUAL RISK |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Utility Risks** | | | | | | Risks associated with KERI infrastructure (Part 1) and vLEI Credentials (Part 2) | | | |
| | vLE software contains undetected bugs or defects that can be exploited by attackers. * | Utility | Security | 5 | 2 | MEDIUM | vLEI software should be tested and/or reviewed or audited for bugs and defects, internally and externally | Mitigation | All vLEI 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 |