

System and Organization Controls (SOC) 3

Relevant to the Trust Services Criteria for
Security Category

For the Period
August 23, 2024 to February 22, 2025

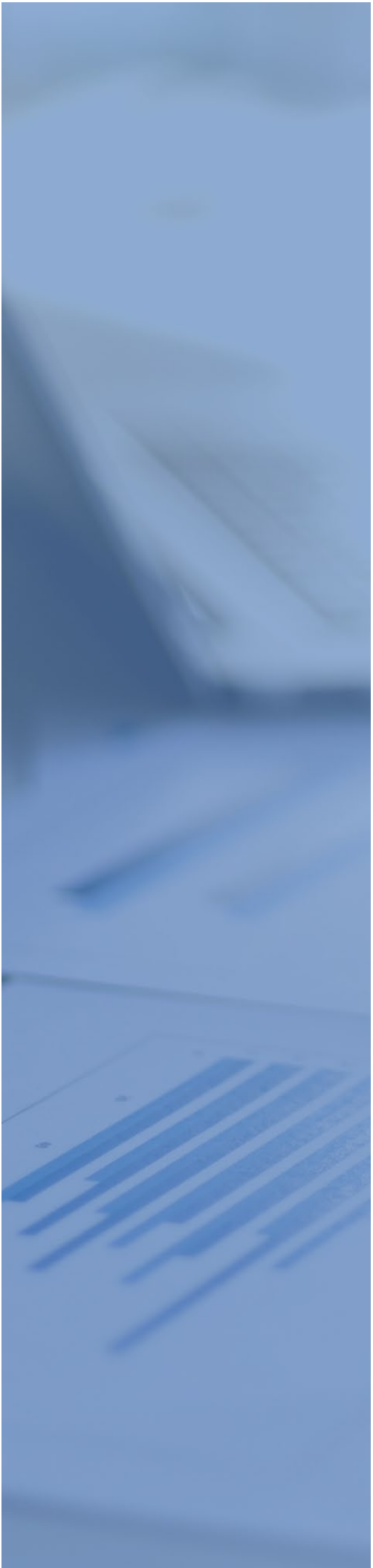
Together with Independent Service
Auditor's Report

Report on Management's Assertion
Related to its System



TABLE OF CONTENTS

I. Independent Service Auditor's Report	3
II. Assertion of ToltIQ, Inc. Management	6
III. Description of ToltIQ Platform	8





Section I

INDEPENDENT SERVICE AUDITOR'S REPORT

TolttIQ, Inc.**Scope**

We have examined TolttIQ, Inc.'s accompanying assertion titled "Assertion of TolttIQ, Inc. Management" (assertion) that the controls within TolttIQ, Inc.'s TolttIQ Platform (system) were effective throughout the period August 23, 2024 to February 22, 2025, to provide reasonable assurance that TolttIQ, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

Service Organization's Responsibilities

TolttIQ, Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that TolttIQ, Inc.'s service commitments and system requirements were achieved. TolttIQ, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, TolttIQ, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective in achieving TolttIQ, Inc.'s service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective in achieving TolttIQ, Inc.'s service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the

future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within ToltIQ, Inc.'s ToltIQ Platform were effective throughout the period August 23, 2024 to February 22, 2025, to provide reasonable assurance that ToltIQ, Inc. service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

JohansonGroup LLP

Colorado Springs, Colorado
March 15, 2025



Section II

ASSERTION OF TOLTIQ, INC. MANAGEMENT

We have prepared the accompanying description of ToltIQ, Inc.'s "Description of ToltIQ Platform " for the period August 23, 2024 to February 22, 2025, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)* (description criteria). The description is intended to provide report users with information about ToltIQ, Inc.'s ToltIQ Platform (system) that may be useful when assessing the risks arising from interactions with ToltIQ, Inc.'s system, particularly information about system controls that ToltIQ, Inc. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

We are responsible for designing, implementing, operating, and maintaining effective controls within ToltIQ, Inc.'s ToltIQ Platform (system) throughout the period August 23, 2024 to February 22, 2025, to provide reasonable assurance that ToltIQ, Inc.'s service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of ToltIQ Platform" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period August 23, 2024 to February 22, 2025, to provide reasonable assurance that ToltIQ, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

ToltIQ, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period August 23, 2024 to February 22, 2025, to provide reasonable assurance that ToltIQ, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

ToltIQ, Inc. Management
March 15, 2025



Section III

DESCRIPTION OF TOLTIQ PLATFORM

COMPANY BACKGROUND

ToltIQ, Inc. is a technology company headquartered in Warren, NJ that is a Generative AI-driven platform for private equity due diligence.

SERVICES PROVIDED

The ToltIQ Platform provides PE firms a way to perform due diligence leveraging Generative AI.

The ToltIQ Platform focuses on the following activities: document ingestion, converting content into vectorized data with embeddings, prompt engineering, leveraging multiple AI models to analyze the data, and producing responses/reports.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

ToltIQ, Inc. designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that ToltIQ, Inc. makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that ToltIQ, Inc. has established for the services. The system services are subject to the security commitments established internally for their services.

System and service commitments are communicated to customers via exhibits A & B of the Software as a Service Evaluation Agreement (Pilot Agreement).

Security Commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings are designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal

COMPONENTS OF THE SYSTEM

The System description is comprised of the following components:

- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data - The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures - The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

ToltIQ, Inc. primarily leverages **Amazon Web Services (AWS)** to host and operate the ToltIQ Platform, relying on AWS's virtual servers, storage, and networking services for scalability and security. In addition to cloud-based infrastructure, ToltIQ, Inc. maintains an inventory of on-premise devices, including desktops and laptops. This inventory documents device ownership and system details, and the organization's network diagram outlines the overall topology of both cloud and local resources. ToltIQ, Inc. is responsible for managing and operating all infrastructure components that support the ToltIQ Platform, ensuring alignment with performance, availability, and security requirements.

Software

The ToltIQ Platform operates on a combination of in-house applications, open-source libraries, and commercial tools for hosting, monitoring, and security. ToltIQ, Inc. selects and manages these software components based on performance, scalability, and security requirements. These include cloud-based services for computing and storage, source control systems, observability platforms, and threat detection solutions.

People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

ToltIQ, Inc. has a staff of approximately 23 organized in the following functional areas:

- **Management:** Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.
- **Operations:** Responsible for ensuring the production infrastructure remains available while also managing and securing its access. Responsible for managing laptops, software, and other technology involved in employee productivity and business operations. Members of the Operations team may also be members of the Engineering team.
- **Engineering:** Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

Data

Data as defined by ToltIQ, Inc., constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

User-Supplied Data - This refers to any data that users upload or submit through the platform. This can include but is not limited to, documents, images, videos, spreadsheets, and other file types. The content of this data is determined by the users and can vary widely. User-supplied data is stored securely in our cloud-based storage systems. We utilize reputable cloud service providers that offer robust security measures, including data encryption both at rest and in transit.

Data is categorized into the following major types of data used by ToltIQ, Inc.

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for ToltIQ, Inc.	<ul style="list-style-type: none"> ● Press releases ● Public website
Internal	Access to internal information is approved by management and is protected from external access.	<ul style="list-style-type: none"> ● Internal memos ● Design documents ● Product specifications ● Correspondences
Customer data	Information received from customers for processing or storage by ToltIQ, Inc. ToltIQ, Inc. must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	<ul style="list-style-type: none"> ● Customer operating data ● Customer PII ● Customers' customers' PII ● Anything subject to a confidentiality agreement with a customer
Company data	Information collected is used by ToltIQ, Inc. to operate the business. ToltIQ, Inc. must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	<ul style="list-style-type: none"> ● Legal documents ● Contractual agreements ● Employee PII ● Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, protect customer data. Additionally, ToltIQ, Inc. has policies and procedures in place for proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

PROCESSES AND PROCEDURES

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by the executive team. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical Security

ToltIQ, Inc.'s production servers are maintained by AWS. The physical and environmental security protections are the responsibility of AWS. ToltIQ, Inc. reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

Logical Access

ToltIQ, Inc. provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privileged access to identified users and to maintain simple and reportable user provisioning and de-provisioning processes.

Access to these systems is split into admin roles, user roles, and no-access roles. User access and roles are reviewed on an annual basis to ensure the least privileged access.

Management is responsible for providing access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing ToltIQ, Inc.'s policies and completing security training. These steps must be completed within 14 days of hire.

When an employee is terminated, Management is responsible for de-provisioning access to all in-scope systems within 4 days of that employee's termination.

Computer Operations – Backups

Customer data is backed up and monitored by the Engineering for completion and exceptions. If there is an exception, Engineering will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS, and physical access is restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer Operations – Availability

ToltIQ, Inc. maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

ToltIQ, Inc. internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

ToltIQ, Inc. utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

Change Management

ToltIQ, Inc. maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

ToltIQ, Inc. has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the ToltIQ, Inc. application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and de-provisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on the underlying hardware.

ToltIQ, Inc. uses automated monitoring services to perform vulnerability scans and engages an external firm to perform annual penetration testing to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the regular incident response and change management process.

BOUNDARIES OF THE SYSTEM

The boundaries of the ToltIQ Platform are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the ToltIQ Platform.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

Common Criteria (to the Security Category)
<p>Security refers to the protection of</p> <ul style="list-style-type: none"> i. information during its collection or creation, use, processing, transmission, and storage, and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of ToltIQ, Inc.'s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of ToltIQ, Inc.'s ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.

- Background checks are performed for employees as a component of the hiring process.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to all relevant policies. They must confirm their understanding of, and responsibility for, adhering to these policies.

Commitment to Competence

ToltIQ, Inc.'s management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

The ToltIQ, Inc. management team must balance two competing interests: continuing to grow and develop in a cutting-edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way ToltIQ, Inc. can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally, any regulatory changes that may require ToltIQ, Inc. to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings with the advisory board are held to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment of Authority and Responsibility

ToltIQ, Inc.'s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

ToltIQ, Inc.'s assignment of authority and responsibility activities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

ToltIQ, Inc.'s success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensure the service organization is operating at maximum efficiency. ToltIQ, Inc.'s human resources policies and practices relating to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.
- New employees are required to review and acknowledge all company policies and sign a confidentiality agreement.

RISK ASSESSMENT PROCESS

ToltIQ, Inc.'s risk assessment process identifies and manages risks that could potentially affect ToltIQ, Inc.'s ability to provide reliable and secure services to our customers. As part of this process, ToltIQ, Inc. maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular ToltIQ, Inc. product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of ToltIQ, Inc.'s system; as well as the nature of the components of the system result in risks that the criteria will not be met. ToltIQ, Inc. addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meet the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, ToltIQ, Inc.'s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

INFORMATION AND COMMUNICATIONS SYSTEMS

Information and communication are an integral component of ToltIQ, Inc.'s internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

ToltIQ, Inc. uses several information and communication channels internally to share information with management, employees, contractors, and customers. ToltIQ, Inc. uses chat systems and email as the primary internal and external communication channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, ToltIQ, Inc. uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. ToltIQ, Inc.'s management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

ToltIQ, Inc.'s management conducts quality assurance monitoring on a regular basis and additional training is provided based on results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in ToltIQ, Inc.'s operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of ToltIQ, Inc.'s personnel.

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

CHANGES TO THE SYSTEM

No significant changes have occurred to the services provided to user entities in the last 3 months.

INCIDENTS

No significant incidents have occurred to the services provided to user entities.

CRITERIA NOT APPLICABLE TO THE SYSTEM

All Common Criteria/Security criteria were applicable to the ToltIQ, Inc.'s ToltIQ Platform system.

SUBSERVICE ORGANIZATIONS

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

Subservice Description of Services

The Cloud Hosting Services provided by AWS support the physical infrastructure of the entity's services.

Complementary Subservice Organization Controls

ToltIQ, Inc.'s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to ToltIQ, Inc.'s services to be solely achieved by ToltIQ, Inc. control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of ToltIQ, Inc.

The following subservice organization controls have been implemented by AWS and included in this report to provide additional assurance that the trust services criteria are met.

Subservice Organization – AWS		
Category	Criteria	Control
Security	CC 6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by the appropriate personnel.
		Closed-circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days unless limited by legal or contractual obligations.
		Access to server locations is managed by electronic access control devices.

ToltIQ, Inc. management, along with the subservice provider, defines the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, ToltIQ, Inc. performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organization(s)

COMPLEMENTARY USER ENTITY CONTROLS

ToltIQ, Inc.'s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to ToltIQ, Inc.'s services to be solely achieved by ToltIQ, Inc. control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of ToltIQ, Inc.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to ToltIQ, Inc.
2. User entities are responsible for notifying ToltIQ, Inc. of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of ToltIQ, Inc. services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize ToltIQ, Inc. services.
6. User entities are responsible for providing ToltIQ, Inc. with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying ToltIQ, Inc. of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.