trisk

Independent Service Auditors' Report on Management's Description of a Service Organization's System Relevant to Security, Confidentiality, Availability and the Suitability of the Design of Controls

As of June 30, 2020

(SSAE 18 - SOC 2 Type 1 Report)

Prepared by: Manoj Jain

www.riskpro.in

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

Independent Service Auditor's Report

To: Management of Trisk Technologies, Inc.

Scope

We have examined the attached Trisk Technologies, Inc. ("Trisk") description of the system titled "Trisk Application Platform as of June 30, 2020" (“Description”) included in Section 3, based on the criteria set forth in the Description Criteria DC Section 200 *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 Report* (“Criteria”) and the suitability of the design of controls included in the Description as of June 30, 2020 to provide reasonable assurance that Trisk’s service commitments and system requirements would be achieved based on the trust service criteria for security, availability and confidentiality set forth in TSP Section 100, 2017 Trust Services Principles and Criteria for Security Availability, Processing Integrity, Confidentiality and Privacy (applicable trust services criteria).

The information included in Section 5, “Other Information Provided by Trisk” is presented by management of Trisk to provide additional information and is not a part of Trisk’s Description. Information about Trisk in Section 5 has not been subjected to the procedures applied in the examination of the Description and of the suitability of the design and operating effectiveness of controls to achieve the Service Organization's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

The Description indicates that Trisk’s controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Trisk’s controls are suitably designed and implemented, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

As indicated in the description, Trisk uses Amazon Web Services (AWS) for data center services and Digital Ocean for monitoring services. The description in Section 3 includes only the controls of Trisk and excludes controls of the various subservice organizations for data center and monitoring services. The description also indicates that certain trust services criteria can be met only if the subservice organization’s controls, contemplated in the design of Trisk’s controls, are suitably designed along with related controls at the service organization. Our examination did not extend to controls of various subservice organizations for data center services.

Service Organization's Responsibilities

Trisk 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 the service commitments and system requirements were achieved.

Trisk has provided the accompanying assertion titled, Trisk’s Management Assertion (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design of the controls described therein to provide reasonable assurance that the service commitments and system requirement would be achieved based on the applicable trust services criteria if operating effectively. Trisk is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization’s service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed to meet the applicable trust services criteria stated in the Description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the presentation of the description based on the description criteria set forth in Trisk’s assertion and on the suitability of the design of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is presented in accordance with the description criteria and (2) the controls are suitably designed to provide reasonable assurance that the service organization’s service commitments and system requirements would be achieved if operating effectively based on the application trust services criteria as of June 30, 2020.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed to meet the applicable trust services criteria. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We did not perform any procedures regarding the operating effectiveness of the controls stated in the description, and, accordingly, do not express an opinion thereon.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs. Because of their nature, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, conclusions about the suitability of the design of the controls to meet the applicable trust services criteria are subject to the risks that the system may change or that controls at a service organization may become ineffective.

Opinion

In our opinion, in all material respects, based on the description criteria described in Trisk’s assertion and the applicable trust services criteria:

a. the description fairly presents the system that was designed and implemented as of June 30, 2020.

b. the controls stated in the description were suitably designed as of June 30, 2020, to provide reasonable assurance that Trisk’s service commitments and system requirements would be achieved if the controls operated effectively as of June 30, 2020, and the subservice organization and user entities applied the controls contemplated in the design of Trisk’ controls as of June 30, 2020.

Description of Controls

The specific controls are presented in the section 4 of our report titled "Trust Services Criteria and Description of Controls"

Restricted Use

This report, including the description of controls in Section 4 of this report, is intended solely for the information and use of Trisk; user entities of Trisk’s systems as of June 30, 2020; and those prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations or other parties
- Internal control and its limitations
- User entity responsibilities, Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

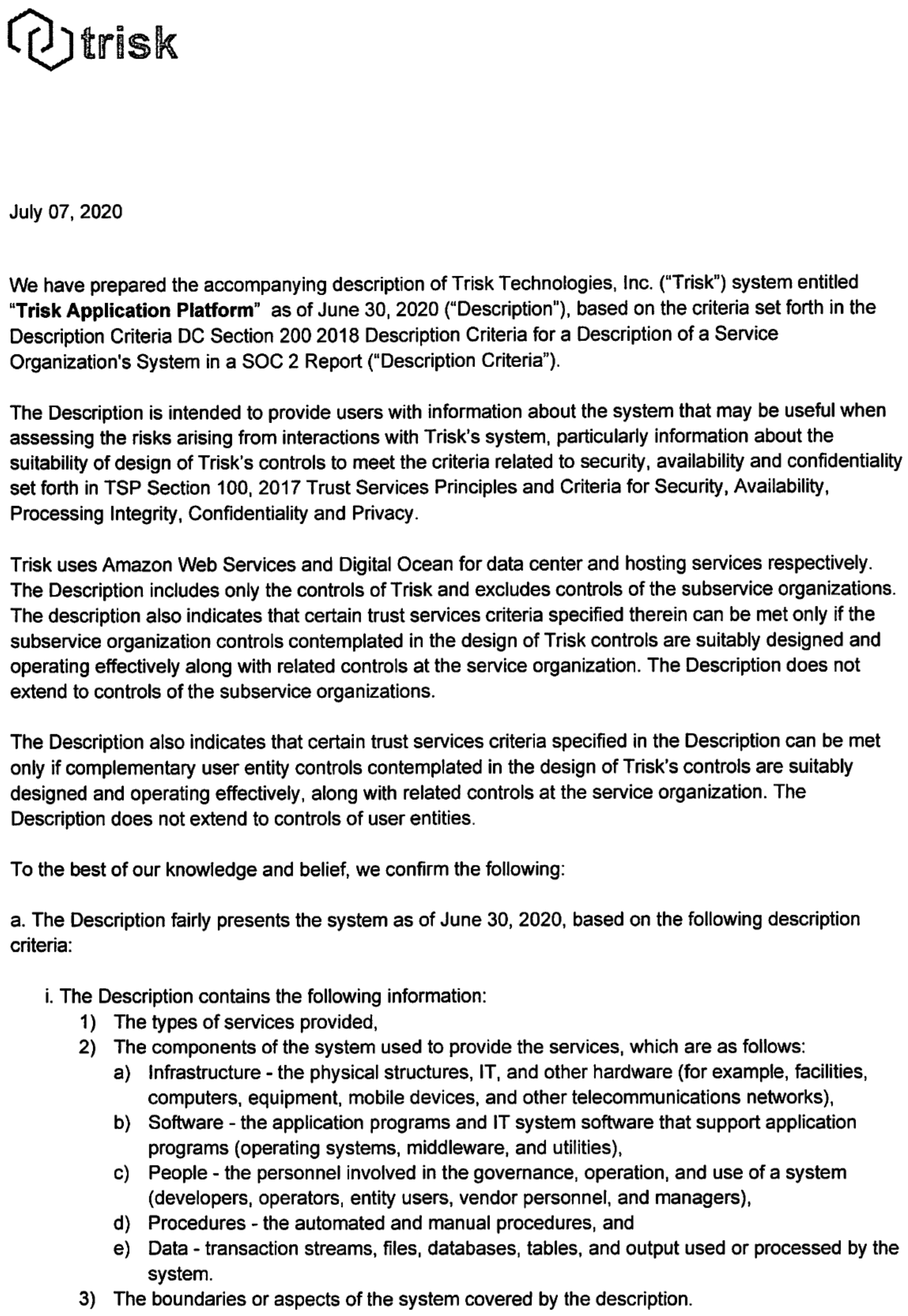
Manoj Jain, CPA
(Colorado Membership Number - 0023943)

July 07, 2020
Mumbai, India

SECTION 2

MANAGEMENT OF TRISK’S ASSERTION

Management of Trisk’s Assertion



July 07, 2020

We have prepared the accompanying description of Trisk Technologies, Inc. (“Trisk”) system entitled “**Trisk Application Platform**” as of June 30, 2020 (“Description”), based on the criteria set forth in the Description Criteria DC Section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (“Description Criteria”).

The Description is intended to provide users with information about the system that may be useful when assessing the risks arising from interactions with Trisk’s system, particularly information about the suitability of design of Trisk’s controls to meet the criteria related to security, availability and confidentiality set forth in TSP Section 100, 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy.

Trisk uses Amazon Web Services and Digital Ocean for data center and hosting services respectively. The Description includes only the controls of Trisk and excludes controls of the subservice organizations. The description also indicates that certain trust services criteria specified therein can be met only if the subservice organization controls contemplated in the design of Trisk controls are suitably designed and operating effectively along with related controls at the service organization. The Description does not extend to controls of the subservice organizations.

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls contemplated in the design of Trisk’s controls are suitably designed and operating effectively, along with related controls at the service organization. The Description does not extend to controls of user entities.

To the best of our knowledge and belief, we confirm the following:

a. The Description fairly presents the system as of June 30, 2020, based on the following description criteria:

i. The Description contains the following information:

1) The types of services provided,
2) The components of the system used to provide the services, which are as follows:
    a) Infrastructure - the physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks),
    b) Software - the application programs and IT system software that support application programs (operating systems, middleware, and utilities),
    c) People - the personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers),
    d) Procedures - the automated and manual procedures, and
    e) Data - transaction streams, files, databases, tables, and output used or processed by the system.
3) The boundaries or aspects of the system covered by the description.

4) For information provided to, or received from, subservice organizations or other parties,
   a) how such information is provided or received and the role of the subservice organization and other parties, and
   b) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.
5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:
   a) Complementary user entity controls contemplated in the design of the service organization's system.
   b) When the inclusive method is used to present a subservice organization, controls at the subservice organization.
6) If the service organization presents the subservice organization using the carve out method,
   a) the nature of the services provided by the subservice organization, and
   b) each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.
7) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons.

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. The controls stated in the Description were suitably designed as of June 30, 2020 to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated as described and if user entities applied the complementary user entity controls, and the subservice organization applied the controls contemplated in the design of Trisk controls.

Sincerely,

Thomas M. Brehmer
CEO

SECTION 3

DESCRIPTION OF “TRISK APPLICATION PLATFORM”

AS OF JUNE 30, 2020

Description of Trisk Application Platform as of June 30, 2020

Background and Overview of Services

Trisk is a SaaS application offered as a platform to enable subject matter experts to interact with clients to streamline data collection and compliance.

Using Trisk's no-code software platform, any person needing to collect data from another person to produce a deliverable can design, implement, launch and run automated custom workflows; without the need for programmers; in hours or days, not weeks or months. Trisk integrates custom forms with co-working functionality, task scheduling, communications and secure data storage, delivering the first end-to-end tool to address the complex efficiency and security challenges of 21st century service providers.

Subservice Organizations

Trisk utilizes the following subservice providers for data center services that are not included within the scope of this examination. However, Trisk's responsibilities for the applications and services running at these cloud services are covered as part of the audit and in scope. Responsibility matrix is defined as part of the SLA and agreements with these sub service organizations.

Amazon Web Services (AWS)

AWS is used for hosting Trisk applications. AWS is a SOC 2 attested company,

The Criteria that relate to controls at the subservice organizations include all criteria related to the Trust Service Principles of Security, Confidentiality and Availability. The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Trisk include:

- The system is protected against unauthorized access (both physical and logical).
- The system is available for operation and use and in the capacities as committed or agreed.
- Policies and procedures exist related to security and availability and are implemented and followed.

Principal Service Commitments and System Requirements

Trisk designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Trisk makes to user entities, the laws and regulations that govern the provision of products and services to its customers, and the financial, operational, and compliance requirements that Trisk has established for the services. Security commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided online.

Trisk establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Trisk's system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.

Components of the System

The System is comprised of the following components:

- Infrastructure including the physical structures, information technology (“IT”) and other hardware,
- Software including cloud subscriptions of application programs and AWS hosting that support application programs,
- People including executives, finance, software development, finance and HR,
- Procedures (automated and manual), and
- Data including transaction streams, files, databases, tables, and output used or processed by the system.

The System boundaries include the applications, databases and infrastructure required to directly support the services provided to Trisk's customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to Trisk's customers are not included within the boundaries of its system.

Boundaries of the System

The specific products and services and locations included in the scope of the report are given below. All other products, services and locations are not included.

Products and Services in Scope

Product

- Trisk Application platform hosted on AWS

Geographic Locations in Scope

Office Location	Address
Development Centre – Ukraine	Seredn'ofontans'ka St, 35, Odessa, Odessa Oblast, 65039, Ukraine

The report excludes all processes and activities that are executed outside above locations. Trisk has a home office in the United States at 518 Almer Road, #4, Burlingame, CA 94010. The USA office is not included in the scope of the report. Unless otherwise mentioned, the description and related controls apply to locations covered by the report.

Description of Control Environment, Control Activities, Risk Assessment, Monitoring and Information and Communication

Control Environment

Trisk’s internal control environment reflects the overall attitude, awareness, and actions of management concerning the importance of controls, and the emphasis given to controls in the Company's policies, procedures, methods, and organizational structure.

The Chief Executive Officer, the Senior Management Team and all employees are committed to establishing and operating an effective Information Security Management System in accordance with its strategic business objectives. The Management at Trisk is committed to the Information Security Management System, and ensures that IT policies are communicated, understood, implemented and maintained at all levels of the organization and regularly reviewed for continual suitability.

Integrity and Ethical Values

Trisk requires directors, officers, and employees to observe high standards of business and personal ethics in conducting their duties and responsibilities. Honesty and integrity are core principles of the company and all employees are expected to fulfill their responsibilities based on these principles and comply with all applicable laws and regulations. Trisk promotes an environment of open communication and has created an environment where employees are protected from any kind of retaliation should a good faith report of an ethics violation occur. Executive management has the exclusive responsibility to investigate all reported violations and to take corrective action when warranted.

Board of Directors / Management

Business activities at Trisk are under the direction of the management. The company is governed by its management headed by its founder Thomas Brehmer as the Founder & Chief Executive Officer ("CEO"). Todd Suchevits is a co-founder and the company's Chief Financial Officer ("CFO") and oversees corporate financial matters. Yuri Vizitei is a co-founder and Chief Technology Officer ("CTO")/Chief Information Security Officer ("CISO") in charge of the company's global development operations playing a key role in technology, strategy and customer management.

Management's Philosophy and Operating Style

The executive management team at Trisk assesses risks prior to entering into business ventures and relationships. The size of Trisk enables the executive management team to interact with operating management on a daily basis.

Risk Management and Risk Assessment

The application of protection measures is based on the risk associated with information assets and the importance of those assets to the organization. As part of this process, threats to security are identified and the risk from these threats is formally assessed.

Trisk has placed into operation a risk assessment process to identify and manage risks that could adversely affect their ability to provide reliable processing for User Organizations. This process consists of management identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks. The executive management team participates in forums and core working groups in industry forums that discuss recent developments.

Information Security Policies

Trisk has developed organization wide information security policies.

Relevant and important security policies are made available to all employees via Google drive or as hard copy policies to new employees. Changes to the information security policies are reviewed by the CISO and approved by CEO prior to implementation.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in business conditions. Trisk management and information security personnel monitor the quality of internal control performance as a routine part of their activities.

Production systems and infrastructure are monitored through service level monitoring tools which monitor compliance with service level commitments and agreements. Reports are shared with applicable personnel and customers, and actions are taken and communicated to relevant parties, including customers, when such commitments and agreements are not met. In addition, a self-assessment scan of vulnerabilities is performed using online scanning service "Intruder.io". Vulnerabilities are evaluated and remediation actions monitored and completed. Results and recommendations for improvement are reported to management.

Information and Communication

Trisk has documented procedures covering significant functions and operations for each major work group. Policies and procedures are reviewed and updated based upon changes and approval by management. Management monitors adherence to Trisk policies and procedures as part of their daily activities.

Trisk management holds status meetings, along with strategic planning meetings, to identify and address service issues, customer problems, and project management concerns. Given the size of the organization, there is no dedicated service manager who is the focal point for communication regarding the service activity. Additionally, management acts as the designated interface with the customer and takes care of processing or systems development issues which affect customer organizations. Electronic messaging has been incorporated into many of Trisk's processes to provide timely information to employees regarding daily operating activities and to expedite management's ability to communicate with Trisk employees.

Electronic Mail (Email)

Communication to Customer Organizations and project teams through email. Important corporate events, employee news, and cultural updates are some of the messages communicated using email. Email is also a means to draw attention of employees towards adherence to specific procedural requirements.

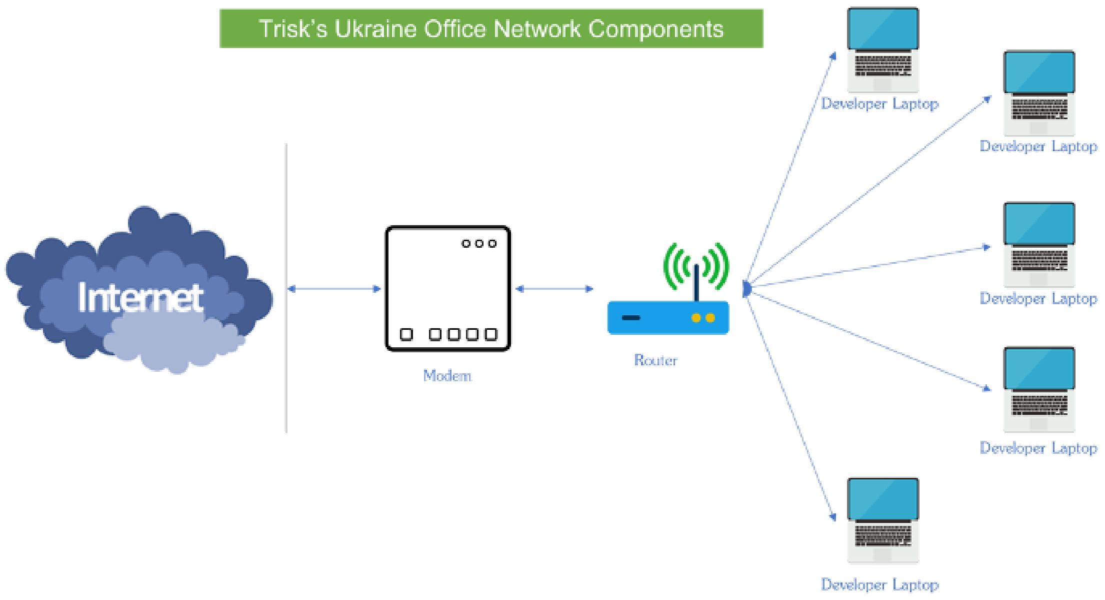
Components of the System

Infrastructure

The infrastructure comprises physical and hardware components of the System including facilities, equipment, and networks.

Network Segmentation Overview

Trisk offices are equipped with the latest hardware, software and networking infrastructure. Offices are linked using high speed communication links. There is no provision for redundancy in networking equipment.



Physical Access
Trisk has its development center in Ukraine. The center is staffed by full-time Individual Entrepreneurs (“IE”), a formal employment status in Ukraine. The entrance is secured with an electronic access control and CCTV surveillance. Physical and Environmental Security of Trisk is controlled and governed by Trisk’s Information Security Management System (“ISMS”) Manual.

All IEs are provided with access cards. These cards open the door lock. Attendance is recorded through electronic access control system. IEs swipe in the access management system to gain entrance to the facility. CCTV is implemented to monitor the activities in secure zones.

ID cards are issued to new personnel, including IEs, based on an access requisition initiated by the Head of Engineering in Ukraine. On separation of personnel from the organization, the Head of Engineering initiates the 'Exit Process'. Based on this, the individual’s privileges in the access control system are revoked.

Fire Extinguishers and smoke detectors are installed at all sensitive points. Regular check on the working condition is done.

Access to the Server Room
Trisk does not have any server rooms.

Software

Firewalls
Trisk is a cloud hosted platform and implements virtual firewall in the form of security groups to control administrative access to the platform. Trisk does not have any physical firewall installation.

Network & endpoint protection / monitoring
Trisk is a cloud hosted platform and performs monitoring by ingesting logs into ELK stack. Apple MacBook’s are provided to IEs in Ukraine for development protection and there is no specific endpoint protection capabilities installed on these devices.

Monitoring

Trisk has devised and implemented adequate monitoring controls to detect unauthorized information processing activities. Critical servers and systems are configured to log user activities, exceptions and information security events. System administrator and system operator activities are logged and reviewed on a periodic basis.

Capacity management controls are put in place to make certain Trisk’s resources are monitored, tuned and projections are made to ensure system performance meets the expected service levels and to minimize the risk of systems failure and capacity related issues.

Patch Management
The development team makes use of updated versions of AWS assets using CI/CD pipeline. Operating system updates are applied as they become available.

Vulnerability Scans & Intrusion Detection/Intrusion Prevention
Online scanning service “Intruder.io” is used for performing vulnerability assessment.

Google suite is used for all inbound and outbound email which provides protection against harmful attachments including viruses and malware.

People

Organizational Structure
The organizational structure of Trisk provides the overall framework for planning, directing, and

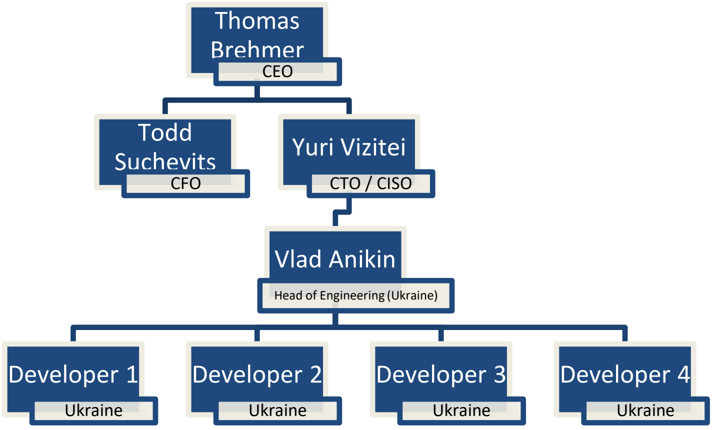
controlling operations.

Thomas Brehmer is responsible for oversight of Trisk. The Trisk Ukraine site is locally managed by Head of Engineering Ukraine.

The management team meets periodically to review plans and performances. Weekly, monthly meetings and calls with senior management are held to review operational, security and business issues, and plans for the future.

Trisk's ISMS manual defines and assigns responsibilities/accountabilities for information security. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

Trisk Organization Chart



Roles and Responsibilities

The following are the responsibilities of key roles.

CEO

The CEO approves and monitors information security strategy, reviews and approves business plans, operational plans and budgets and ensures that security considerations are embedded in plans. The CEO evaluates Trisk's organizational structure, reporting lines, authorities, and responsibilities viz a viz security of information. The CEO provides direction to business planning process and risk assessment and management process; reviews and approves security related policies and procedures pertaining to human resources, information security, and operational processes; appoints Chief Information Security Officer; provides finance and resources to meet objectives and targets; and interfaces with legal counsel to ensure information security strategy is fully compliant with existing laws and regulations.

CISO

- To conduct information security risk assessment and implement risk mitigation plan
- To organize/conduct security reviews and audits
- To organize management reviews of ISMS
- To promote awareness amongst employees on ISMS
- To implement ISMS policies and procedures
- Define and maintain the information security policies

- Prepares and periodically updates ISMS manual needed to improve information security at Trisk
- Implement appropriate controls to protect the confidentiality, integrity, availability, and authenticity of restricted information
- Coordinate a response to actual or suspected breaches in the confidentiality, integrity or availability of critical business information
- Investigate breaches of security policies, controls, and implements additional compensating controls when necessary
- Update Trisk's human resources, legal counsel, procurement and other relevant departments with any updates with regards to information security policy
- Supervise, coordinate and ensure that security measures implemented meet the requirements of the security policy

Commitment to competence

Trisk's formal job descriptions outline the responsibilities and qualifications required for each position in the company. Training needs are identified on an ongoing basis and are determined by current and anticipated needs of the business. Employees and IEs are evaluated on an annual basis to document performance levels and to identify specific skill training needs.

Assignment of Authority and Responsibility

Management is responsible for the assignment of responsibility and delegation of authority within Trisk.

Human Resources Policies and Procedures

Trisk maintains written human resources policies and procedures. The policies and procedures describe Trisk practices relating to hiring, training and development, performance appraisal and advancement and the termination. Human Resource ('HR') policies and practices are intended to inform employees and IEs ("Personnel") on topics such as expected levels of integrity, ethical behavior and competence.

HR policies and procedures are reviewed on periodic basis to ensure they are updated to reflect changes in the organization and the operating environment. Personnel are informed of these policies and procedures upon their hiring and sign an acknowledgement form confirming their receipt. Personnel policies and procedures are documented in the Trisk HR Manual.

New Hire Procedures

New Personnel are required to read Trisk's corporate policies and procedures and sign an acknowledgement form stating that they have read and understand them. Hiring procedures require that the proper educational levels have been attained along with required job-related certifications, if applicable, and industry experience. If a candidate is qualified, interviews are conducted with various levels of management and staff.

Background and reference checks are completed for prospective Personnel prior to employment over phone. Personnel are required to sign Employee Confidentiality Agreements. Any discrepancies found in background investigations result in disciplinary actions, up to and including employee termination.

Performance Evaluation

Trisk has a performance review and evaluation program to recognize Personnel for performance and contributions. Trisk performance evaluation process is also used to help Personnel improve their performance and skill levels. Performance reviews, promotion and compensation adjustments are performed every 12 months.

New Personnel Training

CTO coordinates to provide information security awareness programs to all Personnel as part of new hire training. Records of training are maintained.

Personnel Terminations

Terminations or changes in employment are processed pursuant to the Trisk HR Manual. There are clearly identified and assigned responsibilities with regard to terminations or changes in employment.

Access privileges are revoked upon termination of employment, contract or agreement. In case of a change of employment/engagement role, rights associated with the prior roles are removed and new access privileges are created as appropriate for the current job roles and responsibilities.

Ethical Practices

Trisk reinforces the importance of the integrity message and the tone starts at the top. Every employee, manager, director and IE consistently maintains an ethical stance and supports ethical behavior. Personnel at Trisk encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

Code of Conduct and Disciplinary Action

Trisk has put forward a Code of Conduct and disciplinary process in order to encourage and maintain standards of conduct and ensure consistent and fair treatment for all. Any Trisk employee, IE or contractor whose conduct does not comply with an element of the code of conduct and has been found to have breached the Code is prosecuted as per defined process.

Policies and Procedures

IT policies and operating instructions are documented. Procedures described cover backup, cloud network management, incident management, cloud operations etc.

Help Desk

Trisk makes use of email address jira@trisk.us to log incoming requests as tickets in Jira software. Jira software provides an integrated helpdesk to handle problems and support requirements of users, support users in case of incidents and manage them without disruption to Trisk's business and ensures that changes to any component of Trisk 's information assets and infrastructure are controlled and managed in a structured manner.

Change Management

Trisk has implemented a well-defined change management process to ensure that all changes to the information processing facilities including Trisk platform and cloud security features are managed and controlled. The change management process describes a methodical approach to handle the changes that are to be made to any work product. All the changes need to be subjected to a formal change management process.

Change management covers any change to the information assets of Trisk and includes, but is not limited to, addition/ modification in the application, application components, database structure, DBMS, system and network components, policies and procedures.

Trisk's change management process requires software configuration changes to be tested before deployment into the staging or production environments.

All changes are recorded, approved, implemented, tested and versioned before moving to production environment. The impact of implementing every significant change are analyzed and approved by the CTO before such implementation.

Incident Response and Management

Procedures for incident management, including incident logging, are included in the policy. Users or any other person log all incidents to the Help Desk. The Help Desk personnel study and escalate all security incidents to the designated team for further escalation/resolution. Any event related to security of information assets including facilities and people are termed as an incident.

When an incident is detected or reported, a defined incident response process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures. Root-cause analyses of high severity incidents are performed.

Logical Access

Security Authorization and Administration

Email is sent from Head of Engineering Ukraine to CEO for all new IEs for a new laptop configured with minimum default access to company resources/applications required by Personnel to perform the job duty. Trisk provides manufacturer default configuration for newly procured laptops.

Personnel have admin privileges on their laptops. The ability to create or modify users and user access privileges is not limited.

Access to AWS resources is granted to an authenticated user based on the user's identity through a unique login ID that is authenticated by an associated password. Assets have assigned owners who are responsible for evaluating the appropriateness of access based on job roles.

Privileged access to sensitive resources is restricted to management and Head of Engineering Ukraine. Access to storage, backup data, systems, and media is limited to management and Head of Engineering Ukraine through the use of logical access controls.

Security Configuration

Employees establish their identity to AWS through the use of a valid unique user ID that is authenticated by an associated password. The use of VPN is currently not implemented and the Personnel connect to the AWS cloud infrastructure using their credentials. Remote access is permitted to all Personnel using their credentials.

Passwords are controlled through a password policy and include password complexity requirements. Guest and anonymous logins are not allowed on any laptops. Local administrator privilege is not restricted.

Administrative Level Access

Administrative rights and access to administrative accounts are granted to individuals that require that level of access in order to perform their jobs. All administrative level access, other than to CEO, must be justified to and approved by CTO.

Confidentiality

All agreements with related parties and vendors include confidentiality commitments consistent with company's confidentiality policy (as described in the ISMS Manual).

Secure procedures are established to ensure safe and secure disposal of media when no longer required. The level of destruction or disposal of media would depend on the information or data stored in the media and the criticality of the information as per the information classification guideline.

Backup of Data

Trisk has developed formal policies and procedures relating to backup of data and the same is defined in the backup policy. Suitable backups are taken and maintained.

Trisk has put in place backup processes that define the type of information to be backed up and backup schedule. The backup processes are approved by the CEO and comply with the requirements for business continuity, and legal & regulatory requirements. All backup and restoration logs are maintained for retention periods as defined in the backup procedures.

Users are made aware through adequate training their responsibilities for ensuring backup of required data and information.

Applicable Trust Services Criteria and related Controls

The security, availability and confidentiality trust services categories and Trisk related controls are included in section 4 of this report, “Trust Service Criteria and Description of Controls”.

Trisk has determined that Processing Integrity and Privacy trust services Categories are not relevant to the system.

User- Entity Control Considerations

Services provided by Trisk to user entities and the controls of Trisk cover only a portion of the overall controls of each user entity. Trisk controls were designed with the assumption that certain controls would be implemented by user entities. In certain situations, the application of specific controls at user entities is necessary to achieve relating to the services outlined in this report to be achieved solely by Trisk. This section highlights those internal control responsibilities that Trisk believes should be present for each user entity and has considered in developing the controls described in the report. This list does not purport to be and should not be considered a complete listing of the controls relevant at user entities. Other controls may be required at user entities.

- **Contractual Arrangements**
    - User organizations are responsible for understanding and complying with their contractual obligations to Trisk such as providing input information, review and approval of processed output and releasing any instructions.
- **Other Controls**
    - User Organizations are responsible for ensuring end customer/client privacy.
    - User Organizations are responsible for ensuring that complete, accurate and timely information is provided to Trisk for processing.
    - User Organizations are responsible for their network security policy and access management for their networks, application & data.
    - User Organizations are responsible for working with Trisk to jointly establish service levels and revise the same based on changes in business conditions

SECTION 4

TRUST SERVICES CRITERIA AND DESCRIPTION OF CONTROLS

Trust Services Criteria and Description of Controls

Ref No	Controls Implemented by Trisk
	Control environment
CC1.1	**COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.**
	The entity has code of conduct as part of HR procedures that establishes standards and guidelines for personnel ethical behaviour. Personnel are required to read and accept the entity's code of conduct
	All new Personnel have to read and sign the Confidentiality Agreement/NDA upon joining.
	Customer can provide their issues, complaints or feedback through email to management. Employees/Independent Entrepreneurs ("IE")s can raise their complaints and grievances to Head of Engineering/CTO through email or Slack messaging.
CC1.2	**COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.**
	Management Review Meetings headed by CISO are held every 3 months to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives. Meeting minutes are either maintained as audio recordings or as formal meeting minutes.
	The Management team meets weekly and discuss the business as well as operational issues. These meeting focus on product and customer issues,
CC1.3	**COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**
	Organization charts are established that depict authority, reporting lines and responsibilities for management of its information systems. These charts are communicated to employees and are updated as needed
	Company has Information security related policies and procedures that describes information security processes, practices and organization.
	Information security policy is reviewed and approved by the management at least annually.
	The responsibility of managing information security is assigned to CISO. Allocation of information security responsibility is documented in ISMS manual
CC1.4	**COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**

Ref No	Controls Implemented by Trisk
	The company has documented HR Policies and procedures including recruitment, training and exit procedures.
	Job requirements are documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring and transfer process.
	New employees sign offer letter as their agreement and acceptance of broad terms of employment including a brief description of position and other terms.
	Internal reference checks are conducted by CEO/CTO or the hiring manager through document verification and references checks with the former colleagues or managers provided in the resume. External background screening is not carried out currently.
	Company employs IEs for its software development activities based in Ukraine. These IEs are also responsible for maintenance of the AWS infrastructure
	The new hire training is provided by supervisory role and that includes Information security training. In this training, physical access and security policies would be explained.
CC1.5	**COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**
	Roles and responsibilities are defined in written job descriptions and communicated to Personnel and their managers
	Communication and Information
CC2.1	**COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**
	The management team meets weekly and discuss the business as well as operational issues. These meeting focus on product and customer issues,
CC2.2	**COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**
	System boundaries in terms of logical and physical boundaries are documented. Network diagrams are in place. System boundaries are shared with the customers when it is required.
	Customer responsibilities and appropriate system descriptions are provided in contracts.
	Security policies are published on internal access restricted shared location/Google drive.
	An organizational wide incident management process is in place
	Trisk communicates its commitment to security as a top priority for its customers via contracts.
	All system changes that affect internal users are communicated in a timely manner through email/Slack.
	Customer communication is carried out on a timely manner by CEO/CTO. Currently there is no standard Trisk customer specific escalation matrix since all

Ref No	Controls Implemented by Trisk
	customer communication is handled by CEO/CTO. The support requests from customers are emailed to jira@trisk.io
	CISO is responsible for decisions regarding changes in confidentiality practices and commitments. Operational aspects are handled by Head of Engineering/CTO and they communicate changes to the customers as appropriate.
CC2.3	**COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.**
	Company's security, availability and confidentiality commitments regarding the Trisk platform are included in contracts
	There are no contractual SLAs specified presently with Trisk customers to monitor for uptime and other performance criteria.
	The new hire training includes information security training. In this training the HR, physical access and security policies are explained.
	Trisk customer responsibilities are described in subscription agreements
	Customers can provide their issues, complaints or feedback through email to CEO or CTO. Personnel can raise their complaints and grievances to management.
	Customer responsibilities are described in the customer subscription agreement and in system documentation
	Changes to system boundaries, network systems are communicated to customers, if it impacts their operations
	Incidents impacting external users/customers are communicated to them through emails along with root cause analysis, if required.
	Risk Assessment
CC3.1	**COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**
	Management has a business planning process in place that examines existing objectives and establishes new objectives when necessary.
	Risk assessment/risk rating scales are defined to evaluate and assess the significance of risk. This is part of the risk management framework.
CC3.2	**COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.**
	Policies and procedures related to risk management are developed, implemented, and communicated to personnel.
	A risk assessment is performed annually or whenever there are changes in security posture. As part of this process, threats to security are identified and the risk from these threats is formally assessed.

Ref No	Controls Implemented by Trisk
	Identified risks are rated and get prioritized based on their likelihood, impact, detection and the existing control measures.
CC3.3	**COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.**
	The cloud assets such as EC2 instances and open source software versions which are hosted on AWS are replaced by newer versions as they become available so that there is no explicit need to patch outdated versions. For laptops, the updates and patches are periodically installed as they become available.
	List of all hardware and cloud/AWS assets is maintained as part of asset register.
	Trisk has defined a formal risk management process for evaluating risks based on identified vulnerabilities, threats, asset value and mitigating controls.
CC3.4	**COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.**
	Vendor agreements, including any security, availability and confidentiality commitments, are reviewed by appropriate senior management during the procurement process.
	Monitoring Activities
CC4.1	**COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.**
	Access reviews are currently not happening as it is a small team of five developers and there is very little attrition/employee changes. It is planned that system access reviews for AWS infrastructure will be carried out going forward.
	Vulnerability assessments are performed periodically using security intruder service. Third party VAPT are not carried out.
CC4.2	**COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.**
	AWS VPC Flow / Prometheus / security groups are configured to log events that are reviewed on a periodic basis (weekly)
	Control Activities
CC5.1	**COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.**
	As a small firm, there is no adequate segregation of duties. However, compensating monitoring controls are in place to ensure any internal control failures are detected.
CC5.2	**COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.**

Ref No	Controls Implemented by Trisk
	Policies and procedures related to risk management are developed, implemented, and communicated to personnel.
	AWS Config tool is used for AWS configuration settings. AWS Config tool records configurations of RDS, IAM, S3, EC2 VPC.
CC5.3	**COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**
	The Company has implemented major policies and SOPs across business functions.
	All policies and procedures clearly define the roles, responsibilities and accountability for executing policies and procedures.
	Logical and Physical Access Controls
CC6.1	**The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.**
	Trisk has documented procedure for logical access controls
	Access to AWS resources is granted on least privileges basis as default and any additional access needs to be approved.
	Trisk has established hardening standards for AWS Trisk platform infrastructure that include requirements for implementation of security groups, access control, configuration settings, and standardized policies.
	Cloud/AWS Production assets such as EC2 and security groups (which are the equivalent of firewalls) are hardened according to Industry best practices.
	Physical diagram of networking devices for Ukraine office network include modem and router and is documented.
	Trisk does not allow customers to access its cloud/AWS infrastructure.
	Trisk customer access to usage of Trisk platform hosted on AWS is granted during the customer onboarding process. User credentials for Trisk customers is setup by Trisk's Head of Engineering/CTO against a request from the customer/as per contract.
	Access to Trisk platform (front end application access) for the customer data is restricted to Head of Engineering/CTO. Head of Engineering/CTO have admin rights and can add additional Trisk's users on the customer instances as per business requirements.
	Every Trisk laptop has authentication enabled via unique user ID and password. To access cloud/AWS assets, unique user ID is provided for unique identification of developers and management.
	Cloud infrastructure is configured to use the AWS's identity and access management system (“IAM”). Relevant groups have been added in IAM.
	Direct access to cloud infrastructure is possible only through encrypted SSH access by the Head of Engineering/CTO.
	For AWS console access, multi-factor authentication is implemented.
	The Head of Engineering maintains an up-to-date listing of all software.

Ref No	Controls Implemented by Trisk
	All cloud assets have assigned owners who are responsible for evaluating access based on job roles. The owners define access rights when cloud assets are installed or changed.
	All access to AWS resources is restricted to Head of Engineering/CTO and access must be approved by management. Privileged access is reviewed by CTO on a periodic basis.
	Company does not have office network / Active Directory etc. All user machines are independently monitored by the Head of Engineering on a periodic basis. Authentication on user machines is required as per the password policy.
	Account sharing is prohibited unless approved by management.
	Password policy is set at the local policy level. Passwords are manually set on each developer laptops. These are 7 characters in length with complexity enabled. Passwords are reset every 45-60 days by informing Personnel to reset the password. Passwords for cloud Infrastructure/AWS accounts should be rotated every 45-60 days.
	External access is through security groups that allows only the white listed IP addresses.
CC6.2	**Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.**
	On the day of joining, Head of Engineering provides all necessary access. Employee/IE user accounts are removed from various application and network system as of the last date of employment by Head of Engineering.
	When an employee/IE leaves the organization, the HOE/CISO initiates the 'Exit Process'. HOE/CISO informs CTO within 24 hours to deactivate/delete the user ID from the email system and all applications. An exit checklist is used to ensure compliance with termination procedures.
	User deactivation is done by Head of Engineering within 24 hours after an employee/IE is terminated on the last working day.
	Trisk does not allow non-Personnel to access its systems.
	Currently, the Company does not have any office domain/network. All users are considered external users and access AWS directly.
	Company employs IEs for its software development activities based in Ukraine
CC6.3	**The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives.**
	A role-based security process has been defined within AWS infrastructure based on job requirements.

Ref No	Controls Implemented by Trisk
CC6.4	**The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.**
	Entry to the Ukraine office premises is restricted to authorized Personnel. Physical access control system has been implemented to secure the facilities.
	Physical access to Ukraine office premises is monitored through CCTV installed at key points within the premises.
	All visitors to Ukraine office must be escorted by Trisk Personnel when visiting office facilities.
	Trisk is a cloud hosted platform and does not have any physical servers.
	Upon the last day of employment, physical access is deactivated by CTO. For Ukraine IEs, Head of Engineering deactivates physical access for terminated contractors.
	Personnel in the Ukraine Trisk office are required to return their ID cards on the last day, and all ID badges are disabled.
CC6.5	**The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.**
	Data destruction & data disposal policy is implemented for procedures relating to disposal of information assets / equipment
	All data is erased from laptops and other media prior to destruction/disposal as per the data destruction & data disposal policy
CC6.6	**The entity implements logical access security measures to protect against threats from sources outside its system boundaries.**
	Access to AWS infrastructure is restricted by means of AWS security groups.
	There are no firewalls in office since all users connect directly to cloud infrastructure to do their work. Personnel connect to the local Wi-Fi networks securely from their laptops. However, the Ukraine office router has capability to configure firewall rules and the same is configured.
	The production system at AWS is protected by security groups rules (virtual firewall) set up for the virtual private cloud (VPC) provided by AWS. VPC is used to protect all production system hosted at AWS. Only limited personnel have access to production servers using SSH through a NAT gateway.
	ELK is used to collect application logs and send alerts based on preconfigured parameters. All cloud assets are configured into ELK.
	Incoming connection are accepted from only whitelisted IPs as per AWS security groups
	Access to modify security groups is restricted by management.

Ref No	Controls Implemented by Trisk
	There is no data stored outside production systems for any DR test.
	No confidential output is printed internally in the Ukraine office. No customer confidential data resides in office premises.
	Data is stored in encrypted format as per the data encryption policy.
	Use of removable media is currently not prohibited and all user devices have removable ports enabled as a business policy.
	Connections to the AWS-hosted servers are through authenticated SSH sessions or authenticated secure browser session using HTTPS.
CC6.7	**The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.**
	Trisk policies prohibit the transmission of sensitive information over the internet or other public communications paths unless it is encrypted.
	VPN connections to cloud networks are encrypted.
	External users access applications hosted at cloud infrastructure (AWS) through secure https with SSL/TLS certificates.
	The production system at AWS is protected by security groups rules (virtual firewall) set up for the virtual private cloud (VPC) provided by AWS. VPC is used to protect all production system hosted at AWS. Database access is governed by security group policies and login credentials. Production database can only be accessed from production machines.
	Use of removable media is currently not prohibited and all user devices have removable ports enabled as a business policy.
	Storage for workstations and laptops are currently not encrypted.
	Backup media are encrypted during creation.
CC6.8	**The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.**
	Antivirus software is currently not installed as most of the machines are Mac, which have low vulnerabilities to malware. Trisk is predominantly a cloud services company and limited customer data and/or confidential data resides on the local devices.
	The ability to install software on laptops is currently not restricted based on business reasons.
	Any viruses discovered are reported to CISO by the affected employees.
	System Operations
CC7.1	**To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.**
	Management has defined configuration standards and hardening standards.

Ref No	Controls Implemented by Trisk
CC7.2	**The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.**
	The Prometheus / VPC flow / security groups generates alerts that notify about suspicious activity. Alerts are responded to promptly.
	The management receives requests for support through phones and emails, which may include requests to reset user passwords etc.
CC7.3	**The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.**
	A formal, defined incident management process is documented in the ISMS Manual for evaluating reported events.
	Incidents are reported to the CTO/CEO. These are tracked within Trisk platform / incident tracker spreadsheet.
	Reported incidents are logged in Jira tracker as tickets and include the following details Severity Data and Time of incident Details Status Root Cause (High severity incidents only)
CC7.4	**The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.**
	All security incidents are also reviewed and monitored by the CTO/CISO. Corrective and preventive actions are completed for incidents.
	Change management requests are opened for events that require permanent fixes.
	HR policies include code of conduct and disciplinary policy for employee misconduct.
CC7.5	**The entity identifies, develops, and implements activities to recover from identified security incidents.**
	Root cause analysis is performed for major incidents.
	Change Management
CC8.1	**The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.**
	Trisk has defined its change management and approval processes in its information security policies.
	Software design and development change procedures are documented in the SDLC.
	All change requests are logged and change request ticket created. Major changes are approved by CEO/CTO

Ref No	Controls Implemented by Trisk
	All change requests must be peer reviewed by another programmer for consistency purposes.
	System and regression testing is prepared using approved test plans and test data.
	Software code repository Gitlab is used
	Software development changes are tested through unit testing followed by UAT. Each of these activities are captured & monitored in change requests. Test plans are used for testing.
	There is a formal release process for releasing builds. Release notes contain features that are part of the release. The testing team does the complete testing of the release. On receipt of sign off mail from the CTO, the release is deployed on Cloud/AWS production servers.
	Separate environments are used for development, testing, and production. Developers do not have the ability to make changes to software in testing or production.
	All change requests are submitted with implementation and rollback plans.
	The change management process has defined roles and assignments thereby providing segregation of roles in the change management process.
	A process exists to manage emergency changes. Emergency changes, due to their urgent nature, may be performed without prior review.
	Dummy data is currently used for testing. If customer data is used for testing, it would be obfuscated before being used in testing.
	Risk Mitigation
CC9.1	**The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.**
	Trisk has a documented BCP and DR plan and documentation to be used in the event of an event necessitating Trisk infrastructure recovery.
	Business continuity and disaster recovery plans, including restoration of backups, are planned to be tested on an annual basis.
CC9.2	**The entity assesses and manages risks associated with vendors and business partners.**
	New third-party service providers are selected based on a vendor selection process. Security risk assessment is a key part of the vendor selection process. Company requires all key subservices to be compliant with security certifications and attestations such as ISO 27001, SOC1 or SOC2.
	Company obtains and reviews compliance reports and certificates such as PCI DSS, ISO 27001, SOC1 or SOC2 for its key vendors. Opinion section and relevant controls are reviewed for any exceptions. This is part of vendor monitoring.

Ref No	Controls Implemented by Trisk
	A formal contract is executed between Company and third-party service providers before the work is initiated. Agreement includes terms on confidentiality, responsibilities of both parties.
	A confidentiality agreement is signed by all Personnel at the time of joining. In addition, NDAs are signed with third-parties wherever required.
	ADDITIONAL CRITERIA FOR AVAILABILITY
A1.1	**The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.**
	The Company monitors system processing capacity and usage and takes correction actions to address changing requirements Processing capacity is monitored by Prometheus and logs are monitored on an ongoing basis.
	Processing capacity for cloud infrastructure for AWS is monitored by Prometheus on an ongoing basis.
A1.2	**The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.**
	Environmental controls (fire extinguishers, fire sprinklers and smoke detectors) have been installed to protect perimeter area. There are detective controls in place as well such as CCTV installed.
	Vendor warranty specifications such as access card systems, CCTV and HVAC are complied with and tested to determine if the system is properly configured.
	Backup policy is defined in the information security policies
	Automated backup systems are in place to perform scheduled differential and full backup of production systems and internal office data.
	Data backups are stored on the cloud and the process is monitored for completion. If there are failures, the data backup is restarted.
	No backups are performed on external hard drives or tapes.
A1.3	**The entity tests recovery plan procedures supporting system recovery to meet its objectives.**
	Disaster recovery and business continuity plans and procedures for various disruption scenarios are documented.
	Business continuity plans, including restoration of backups, are planned to be tested at least annually.
	ADDITIONAL CRITERIA FOR CONFIDENTIALITY
C1.1	**The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.**
	Trisk establishes written policies related to retention periods for the confidential information it maintains.

Ref No	Controls Implemented by Trisk
	Trisk securely destroys or deletes all data as soon as it is no longer needed.
C1.2	**The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.**
	Trisk establishes written policies related to retention periods for the confidential information it maintains. Trisk securely destroys or deletes all data as soon as it is no longer needed.

SECTION 5

OTHER INFORMATION PROVIDED BY TRISK

Other Information Provided by Trisk

The information provided in this section is provided for informational purposes only by Trisk. Independent Auditor has performed no audit procedures in this section.

Disaster and Recovery Services

The AICPA has published guidance indicating that business continuity planning, which includes disaster recovery, is a concept that addresses how an organization mitigates future risks as opposed to actual controls that provide user auditors with a level of comfort surrounding the processing of transactions. As a result, a service organization should not include in its description of controls any specific control procedures that address disaster recovery planning. Therefore, Trisk's disaster recovery plan descriptions of control procedures are presented in this section.

Since Trisk is a cloud hosted platform, the application is capable of hosting in multiple regions and across availability zones (AZ). Trisk would make use of Continuous Integration / Continuous Deployment as means to quickly spin up the Trisk application platform in a different region or AZ in case need arises.