VISO TRUST

System and Organization Controls 3 (SOC 3) Report

Report on VISO Trust's Description of Its Automated Cyber Due Diligence Platform System Relevant to Security and Availability

For the period June 1, 2022 to August 31, 2022

VISO Trust
Automated Cyber Due Diligence Platform System

Table of Contents

Management's Report of its Assertions on the Effectiveness of Its Controls over the Automated Cyber Due Diligence Platform System Based on the Trust Services Criteria for Security and Availability

VISO TRUST

Management's Report of its Assertions on the Effectiveness of Its Controls over the Automated Cyber Due Diligence Platform System Based on the Trust Services Criteria for Security and Availability

We, as management of, VISO Trust are responsible for:

- Identifying the Automated Cyber Due Diligence Platform System (System) and describing the boundaries of the System, which are presented in *Attachment A*
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in *Attachment B*
- identifying, designing, implementing, operating, and monitoring effective controls over the Automated Cyber Due Diligence Platform System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period June 1, 2022 to August 31, 2022, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security and availability set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

VISO Trust

Report of Independent Accountants

Building a better working world

Ernst & Young LLP
Frost Bank Tower
Suite 1901
111 West Houston Street
San Antonio, TX 78205

Tel: +1 210 228 9696
Fax: +1 210 242 7252
ey.com

Report of Independent Accountants

Scope:
We have examined management's assertion, contained within the accompanying *Management's Report of its Assertions on the Effectiveness of Its Controls over the Automated Cyber Due Diligence Platform System Based on the Trust Services Criteria for Security and Availability* (Assertion), that VISO Trust's controls over the Automated Cyber Due Diligence Platform System (System) were effective throughout the period June 1, 2022 to August 31, 2022, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security and availability (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

VISO Trust uses Amazon Web Services (AWS) to provide physical security and environmental safeguard services and hosting services and Google Workspace to provide communication, storage, and collaboration services (subservice organizations). The Description of the boundaries of the System (Attachment A) indicates that VISO Trust's controls can provide reasonable assurance that certain service commitments and system requirements, based on the applicable trust services criteria, can be achieved only if AWS' and Google Workspace's controls, assumed in the design of VISO Trust's controls, are suitably designed and operating effectively along with related controls at the service organization. The Description presents VISO Trust's system and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS and Google Workspace. Our examination did not extend to the services provided by AWS and Google Workspace and we have not evaluated whether the controls management assumes have been implemented at AWS and Google Workspace have been implemented or whether such controls were suitably designed and operating effectively throughout the period June 1, 2022 to August 31, 2022.

AWS and Google Workspace have descriptions of the services used by the System in their respective SOC reports, which include the aforementioned complementary controls. This report should be read in conjunction with the AWS and Google Workspace SOC reports.

Management's Responsibilities
VISO Trust's management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Automated Cyber Due Diligence Platform System (System) and describing the boundaries of the System
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of the system

- Identifying, designing, implementing, operating, and monitoring effective controls over the Automated Cyber Due Diligence Platform System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement

Our Responsibilities
Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA") and in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of VISO Trust's relevant security and availability policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating VISO Trust's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

We are required to be independent of VISO Trust and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements related to our examination agreement.

We have complied with such independence and other ethical requirements and applied the AICPA's Statements on Quality Control Standards.

Inherent limitations:
Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve VISO Trust's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal

control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion:
In our opinion, VISO Trust's controls over the system were effective throughout the period June 1, 2022 to August 31, 2022, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria, if the subservice organizations applied the controls assumed in the design of VISO Trust's controls throughout the period June 1, 2022 to August 31, 2022.

Restricted use
This report is intended solely for the information and use of VISO Trust and users of the Automated Cyber Due Diligence Platform System and is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst + Young LLP

October 14, 2022

Attachment A

VISO Trust's Description of Its Automated Cyber Due Diligence Platform System Relevant to Security and Availability for the Period June 1, 2022 through August 31, 2022

Attachment A — VISO Trust's Description of Its Automated Cyber Due Diligence Platform System Relevant to Security and Availability for the Period June 1, 2022 through August 31, 2022

Company Overview and Background

VISO Trust is a Software as a Service (SaaS) Company launched in 2020 offering the VISO Trust Platform to its customers. The VISO Trust Platform provides automated security due diligence and third-party cyber risk management to its clients. It uses patented technology and is the industry's first AI-based third-party due diligence platform. VISO Trust's primary aim is to help companies make informed risk decisions quickly and easily. It has a rapidly growing set of customers, ranging from tech companies to Fortune 500 enterprises, across consumer-facing and business-to-business industries like banking, automotive and retail.

Overview of the VISO Trust Platform

VISO Trust's core service is the VISO Trust Platform. This third-party risk management platform delivers rapid security intelligence to modern companies so that they can quickly and easily assess and manage third parties and make critical risk decisions early in the procurement process.

Key Terms in the Platform:

Assessment: An automated security due diligence and evaluation of risk using curated Artificial Intelligence (AI) and document heuristics that is patented technology to the VISO Trust Company.

Relationship: A continuous record of the association of a Client organization and a Third Party.

Artifacts: A general term to encompass data that is collected as part of the assessment.

Organization: It is used to associate users and relationships to a Client tenancy and centralize its configuration.

Business Case: The context of how business is conducted between the Client and the Third Party. This determines the attack surface in the VISO Trust risk model.

Documents: A subset of artifacts, more specifically referring to security documents required for a security assessment and uploaded by the Client or Third Party into the VISO Trust Platform.

Potential Risk: Also known as inherent risk, potential risk is the assessed and total risk possible before a Company has made any efforts to resolve and mitigate risk factors with security controls and changes to their processes.

Residual Risk: The risk that remains after a Company has made efforts to mitigate and eliminate potential risk factors.

Lifecycle: The entirety of the relationship between Client and Third Party, from creating a relationship, to starting and completing an initial assessment, to managing a relationship by updating expiring documents as needed and recertifying assessments on a scheduled basis or terminating a relationship.

Manual Recertification: VISO Trust sends reminders to the Business Owner and Subscribers when the recertification period approaches, and the Client starts a re-assessment manually.

Automatic Recertification: VISO Trust automatically starts a re-assessment of the Third Party when the recertification window approaches.

System Roles in the Platform:

Client: The VISO Trust customer contracted to use the TPRM service.

Third Party: The Company either in the process of being procured or in need of management by the Client organization in order to provide a service or product.

Business Owner: The primary Client business contact in a relationship. This contact is most familiar with the specificities of the business case, and appropriately communicated with or involved in the lifecycle of a relationship.

Subscriber: A Client contact who receives a subset of relationship lifecycle event notification and email messages.

Assessment Creator: The Client contact in a relationship who creates the assessment in the VISO Trust Platform. This contact receives relationship lifecycle event notifications as well as access to make changes in the platform.

System Workflow Lifecycle:

Creating a Relationship: The Client creates and defines a relationship on the Platform between their Company and a Third Party.

Starting an Assessment: The Client triggers an assessment of a Third Party leveraging the context of the defined relationship and optionally including Client submitted artifacts, public resources or an automated notification to the Third Party with an information request for security due diligence.

Responding to an Assessment: The Third Party uploads the required documents and information for the assessment to the Platform.

Managing a Relationship: Once a Third Party has been onboarded into the VISO Trust Platform, the relationship is continuously and systematically monitored for expiring artifacts, changes in relationships, and recertification assessment due dates to keep risk insights up to date.

Recertification Assessment: After an initial assessment of a Third Party has been completed and they have been onboarded into the VISO Trust Platform, Client organizations have the choice to manually or automatically reassess the Third Party on a set date. This reassessment process is referred to as recertification.

The VISO Trust Platform has three key features:

⇨ Turnkey Due Diligence

An automated system that allows companies to quickly and easily assess third parties. There is no implementation, and companies can instantly access risk intelligence for any number of third parties and instantly align with industry standards and frameworks such as National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), American Institute of Certified Private Accountants (AICPA), System and Organizational Controls (SOC), Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and more.

⇨ Document Intelligence

Assessments are delivered using curated AI and document heuristics by an expert team, without any user interaction.

⇨ Lifecycle Automation

Risk is kept up to date and accurate with continual monitoring of vendor documents and data. VISO Trust's automated tracking and communication system eliminates a Company's need to go back and forth between their vendors, and notification features alert companies to necessary information and critical changes.

Components of System

The components of the system used to provide the services are described in the sections below. They include:

- Infrastructure (the physical and hardware components including Physical structures, IT, equipment, and other hardware)
- Software (the programs and operating software of the system including operating systems, databases, applications and utilities)
- People (the personnel involved in governance, operation, and use of the system, procedures involved in the operation of a system)
- Data (information used and supported by a system including transaction streams, files, databases, and tables etc.).

- Procedures (corporate policies or standards, which have been deployed to provide guidelines for management and employees to ensure security and availability commitments)

Infrastructure & Software

The VISO Trust platform operates as a multi-tenant SaaS web application hosted in AWS. The application runs as a horizontally scalable, container-based application. VISO Trust makes use of multiple AWS availability zones to ensure a high level of availability. The Platform must be accessed by clients via HTTPS with TLS 1.2 and higher. AWS-hosted, internal-use-only tools are accessed by VISO Trust personnel using a secure Virtual Private Network (VPN) connection.

VISO Trust utilizes Cloudflare for Cloud Content Delivery Network (CDN) and Web Application Firewall (WAF) protection of its hosted platform. VISO Trust also utilizes Google Workspace for corporate productivity and email and Postmark for transactional email. Okta is the identity provider for the web application as well as single sign-on (SSO) for VISO Trust personnel.

Customer data is encrypted at rest and securely stored in a fault-tolerant database, hosted by Amazon Relational Database Service (RDS) in multiple availability zones. Additionally, documents that are uploaded by customers or third parties are securely stored in Amazon Simple Storage Service (S3).

VISO Trust AWS infrastructure is managed programmatically using Terraform, all revisions are tracked using an industry-standard source control system, and all changes are peer reviewed prior to being deployed to production infrastructure. As a result, a comprehensive, and accurate inventory of virtual assets is available for review.

VISO Trust has built and maintains multiple, logically separated environments that are used throughout the release lifecycle. The production environment is used by their customers and is treated with the greatest level of security and confidentiality. The development environment is used internally to develop and test changes prior to being released to customers.

VISO Trust utilizes the following services and tools to host the application, support customers, and protect their intellectual property.

System / Application	Category	Description
AWS	Infrastructure	Industry leading cloud hosting provider that is used to host the application and all customer data.
Cloudflare	Infrastructure	Cloudflare-owned, globally distributed network of caching servers with application protection. Cloud CDN And WAF Protection.

Elasticsearch	Infrastructure	All VISO Trust infrastructure, security, and web app logs are stored and cataloged within Elasticsearch.
Honeycomb	Infrastructure	Honeycomb is a cloud-hosted observability platform that allows VISO Trust to analyze and inspect the performance of various components of the web application.
Google Workspace	Productivity	Corporate productivity, email, calendar and meeting platform.
JIRA	Productivity	The JIRA ticketing system is used internally for tracking all code or infrastructure changes that are made to the application, user access management, personnel onboarding and offboarding, and customer service support requests.
Confluence	Productivity	Confluence is used by VISO Trust personnel to allow easy creation of documentation and how-to articles for internal processes and procedures.
Slack	Productivity	Slack is used for internal, real-time communication between VISO Trust associates and is also offered to customers as an avenue for support by utilizing the ability for a Slack channel to have external organizations.
Okta	Authentication	Identity provider platform used for multi -factor authentication and SSO functionality.
1Password	Security	Credential storage tool that is used by all VISO Trust associates to securely store all passwords that provide access to both internal and external VISO Trust resources and platforms.
JAMF	Security	JAMF is a cloud-hosted service that gives us remote wipe, policy enforcement, encryption, screen lock capabilities for all VISO Trust owned Apple devices.
GitHub	Development	GitHub is used to securely store all VISO Trust source code, enforce code peer review requirements, and provide a comprehensive Continuous Integration/Continuous Delivery (CI/CD) pipeline.
Terraform Cloud	Development	Terraform Cloud is used to allow infrastructure changes to be written as code, stored in source control, and peer reviewed prior to the change being made to the production infrastructure.

People
VISO Trust has established an organization chart that defines organizational roles, reporting lines and authorities. The following divisions are responsible for providing services related to the VISO Trust platform: Product, Technology, Finance, People Operations, Sales, and Third-Party Audit Operations & Annotation, and Internal Audit. These divisions report to either the Chief Executive Officer (CEO) or the Chief Technology Officer (CTO).

Executive Management: Responsible for overseeing Company-wide directives, activities, and accomplishing high-level strategic goals including information security program and overall security maturity of the business.

Product: Responsible for functions related to product feature development, organization, and research including user experience, product design and scope.

Technology: Composed of multiple teams, this division is responsible for developing VISO Trust's features, infrastructure engineering, system monitoring, security incident response and daily IT troubleshooting tasks.

Finance: Responsible for overseeing financial activities and directives, preparing financial reports and summaries, forecast future growth, and handles day-to-day accounting operations.

People Operations: Responsible for day-to-day task support for management, talent recruitment and retention, and HR-related policies, practices, and processes also including compensation, employee benefits, performance management, employee relations, training, and development.

Sales: Primarily responsible for building and scaling VISO Trust's go-to-market capabilities, driving new customer revenue goals, maintaining client satisfaction and relationships, and closing SaaS subscription revenue sales.

Third Party Audit Operations & Annotation: Responsible for conducting and reporting on domestic and global third-party risk assessments, documenting assessment procedures for subsequent automation, analyzing security program text annotations to ensure quality of conclusions drawn by automated assessments, and assist in coordinating VISO Trust's own due diligence in compliance-related matters as its Technology Compliance team. The team reports to the CEO and serves as a bridge between internal / external audit and the technology teams and is responsible for articulating business-related Technology and security/ availability initiatives to management and recommending and assisting in implementing appropriate compliance frameworks.

Internal Audit: The team reports to the CEO and is authorized to examine internal controls, risk management and governance processes and hence provides an independent and objective conclusion of the assessments performed to validate design and operating effectiveness of VISO Trust's internal controls.

Procedures
VISO Trust has detailed information security and availability policies and procedures which were designed to align with ISO 27001, NIST CSF and other prominent frameworks. These policies and procedures (related to the services provided) include procedures by which service activities are initiated, authorized, performed, and delivered and reports or other information is prepared.

The following list illustrates the security and availability program components/ related policies and procedures in place to address those components. These procedures have been documented and made available to applicable team members and are reviewed at least on an annual basis by the Executive Management team members.

- ⇨ Information Security Policy
- ⇨ Asset Management
- ⇨ Access Management
- ⇨ Personnel Security
- ⇨ Performance Evaluation
- ⇨ Change Management
- ⇨ Network Security
- ⇨ Data Security
- ⇨ Secure Development
- ⇨ Vulnerability Management
- ⇨ Configuration Management
- ⇨ Risk Management
- ⇨ Vendor Risk Management
- ⇨ Logging & Monitoring
- ⇨ Information Security Incident Response
- ⇨ Business Continuity
- ⇨ Capacity Management
- ⇨ Data Handling, Retention and Disposal
- ⇨ Software Development & Acquisition Lifecycle

Data
VISO Trust Customer Data (including Platform Customer Third Party Risk Management Program Data, Platform Customer Artifact Data, Platform Vendor Artifact Data, Client Communication Data (including emails and Slack records)) platform audit logs are managed, processed, and stored in accordance with relevant data protection compliance requirements and with specific requirements formally established in customer contracts. Customer data is treated as confidential (and sensitive for some information types), according to the Data Handling, Retention and Disposal Policy that defines the minimum protection requirements for data based on its classification.

Customer Data in production, while at rest, is encrypted via AES 256 AWS KMS using Customer (VISO Trust) Managed Keys. Further, production system information that is transmitted over public networks is encrypted using at least TLS protocol version 1.2 or higher. Customer Data is maintained in protected systems where active monitoring is enabled and configured to

ensure security. Data is retained and subsequently destroyed in accordance with the Data Handling, Retention and Disposal Policy and based on customer commitments.

Complementary Subservice Organization Controls

The customer – servicing production environment is hosted in AWS, which acts as a subservice organization to VISO Trust. AWS maintains the physical and environmental controls on which VISO Trust relies to protect its systems. VISO Trust also uses Google Workspace for communication, storage, and collaboration purposes and in this way Google also acts as a subservice organization to VISO Trust. To validate the continuing operating effectiveness of the AWS and Google controls upon which VISO Trust relies, management obtains and reviews the independent security and availability audit/ assessment reports on at least an annual basis (to assess compliance). Investigations and discussions are performed for any identified exceptions. While monitored by VISO Trust, AWS hosting, and Google storage and transmission related controls are not included in the scope of this examination.

The following table presents the applicable trust services criteria that are intended to be met by controls at AWS and Google, alone or in combination with controls at VISO Trust, and the types of controls expected to be implemented at AWS, Google, to achieve VISO Trust's service commitments and system requirements based on the applicable trust services criteria.

Controls expected to be Implemented by Subservice organizations	**SSO**
The subservice organization is responsible for managing logical access to the underlying systems, network, virtualization management, and storage devices for its cloud hosting services where the VISO Trust systems or data reside.	AWS, Google Workspace
The subservice organization is responsible for restricting physical access to systems, data center facilities and protected information assets (for example, back-up media storage and other system components including firewalls, routers, and servers) to authorized personnel to meet the entity's objectives.	AWS, Google Workspace
Further, the subservice organization is responsible for implementing environmental security controls to ensure that critical information technology infrastructure is protected from environmental threats.	AWS, Google Workspace
The subservice organization is responsible for implementing procedures to ensure secure destruction of decommissioned equipment or electronic media with VISO Trust information.	AWS, Google Workspace
The subservice organization is responsible for maintaining data confidentiality and integrity by implementing cryptographic controls i.e., ensuring encryption of data during transit and rest.	AWS, Google Workspace

The subservice organization performs regular vulnerability and penetration testing assessments on the information systems and supporting network and vulnerabilities identified are reviewed, prioritized, and resolved as per the defined time frame. Further, vulnerability assessment tools are periodically updated to the latest patches and signature definition files.	AWS, Google Workspace
The subservice organization is responsible for evaluating security events to determine whether they could or have resulted in a failure of the entity to meet its objectives and if so, take actions to address such events and failure	AWS, Google Workspace
The subservice organization is responsible for maintaining and updating security patch levels of VISO Trust servers and ensuring that changes (including emergency/non-routine and configuration) to existing IT infrastructure resources are logged, authorized, tested, approved, and documented.	AWS, Google Workspace
The subservice organization is responsible for backing up the production systems and monitoring the backups for successful replication across multiple data centers.	AWS, Google Workspace
The subservice organization is responsible to perform tests supporting system recovery (disaster recovery and business continuity planning and testing) to meet its availability commitments.	AWS, Google Workspace

Attachment B

Principal Service Commitments and System Requirements

Attachment B - Principal Service Commitments and System Requirements

Commitments to user entities are documented and communicated in the security overview and terms of service provided on the VISO Trust website, customer agreements, as well as in the description of service offerings provided online. Security and Availability commitments are standardized and include but are not limited to, the following:

- ⇨ Native support for multi-factor authentication, enterprise SSO and Role-Based Access Control (RBAC)
- ⇨ CDN-based Web Application Firewall protection
- ⇨ Industry standard encryption in transit and at rest
- ⇨ Comprehensive incident response and Security Information and Event Management (SIEM) infrastructure monitored 24x7x365
- ⇨ Continuous security testing in development lifecycle (both software components and infrastructure code)
- ⇨ Robust performance and availability infrastructure monitored 24x7x365
- ⇨ Frequent penetration testing

VISO Trust establishes operational requirements that support the achievement of security and availability commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in VISO Trust system policies and procedures, system design documentation and contracts with customers. Information security policy and procedures 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.

In accordance with the assertion and description criteria, the aforementioned service commitments and system requirements are the principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users in each individual case.