Crowe

Smart decisions. Lasting value.™

System and Organization Controls Report SOC 3®

Independent Service Auditor's Report on Controls at a Service Organization Relevant to Security and Availability

Related to Chainalysis, Inc.'s Reactor and KYT Systems

Under the AICPA, Statement on Standards for Attestation Engagements No. 18 (SSAE No. 18), Section AT-C 205, *Examination Engagements*

For the Period June 1, 2021 to November 30, 2021

Chainalysis

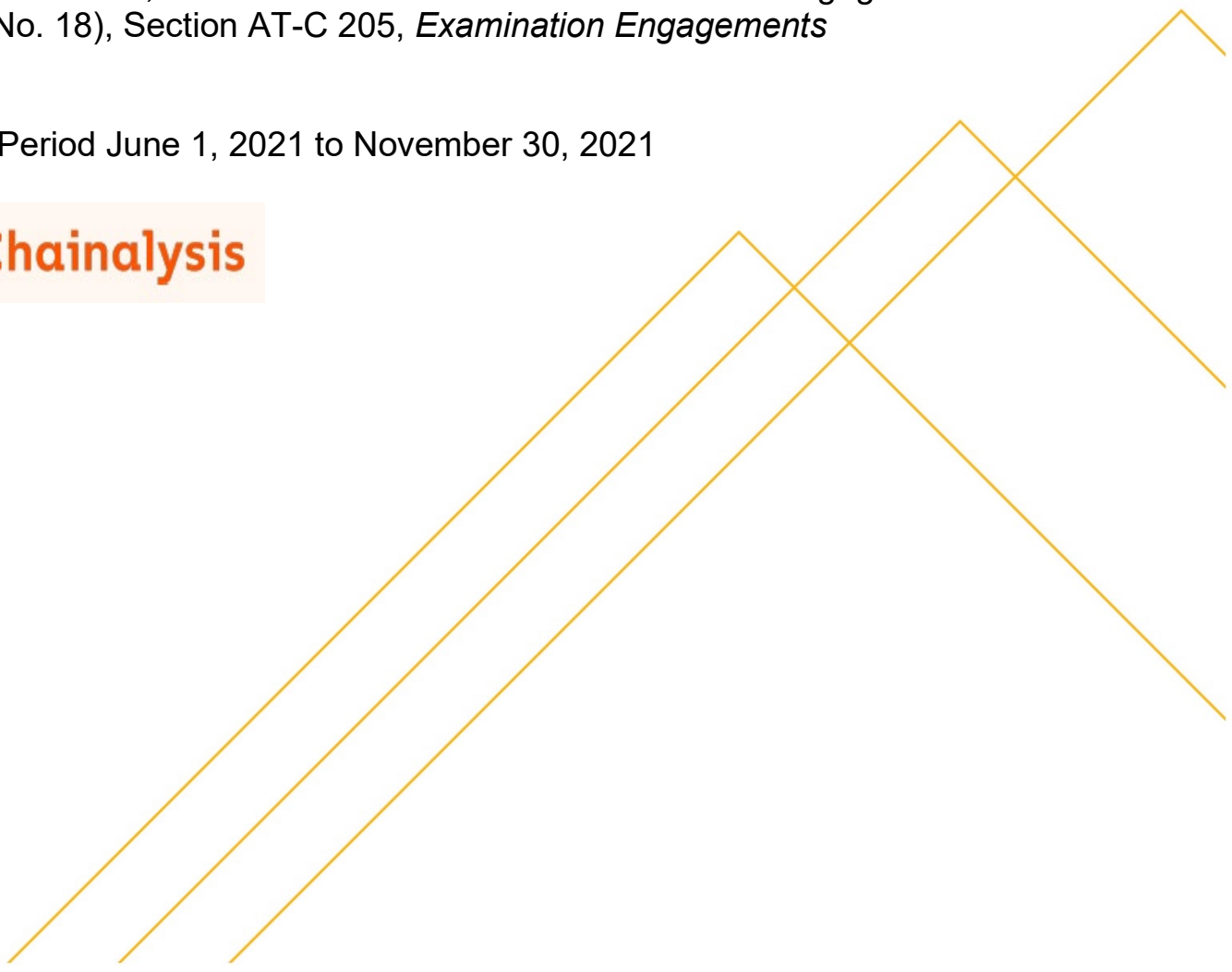


Table of Contents

SECTION I: Independent Service Auditor’s Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To Chainalysis, Inc.

Scope

We have examined Chainalysis, Inc. (Chainalysis or service organization) accompanying assertion titled "Assertion of Chainalysis, Inc.' Management" (assertion) that the controls within Chainalysis' Reactor and KYT systems (system) were effective throughout the period June 1, 2021 to November 30, 2021, to provide reasonable assurance that Chainalysis' service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA*, Trust Services Criteria).*

Service Organization's Responsibilities

Chainalysis 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 Chainalysis's service commitments and system requirements were achieved. Chainalysis has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Chainalysis is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the controls were not effective to achieve Chainalysis' service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the systems were effective to achieve Chainalysis' service commitments and system requirements based on the applicable trust services criteria

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

Inherent Limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Chainalysis' Reactor and KYT systems were effective throughout the period June 1, 2021 to November 30, 2021, to provide reasonable assurance that Chainalysis' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Crowe LLP

South Bend, Indiana
April 4, 2022

SECTION II: Assertion of Chainalysis, Inc.’s Management

Chainalysis

April 4, 2022

ASSERTION OF CHAINALYSIS, INC.'S MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Chainalysis, Inc.'s (Chainalysis or service organization) Reactor and KYT systems throughout the period June 1, 2021 to November 30, 2021, to provide reasonable assurance that Chainalysis' service commitments and system requirements relevant to Security and Availability (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2021 to November 30, 2021, to provide reasonable assurance that Chainalysis' service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Chainalysis' objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

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

We assert that the controls within the system were effective throughout the period June 1, 2021 to November 30, 2021, to provide reasonable assurance that Chainalysis' service commitments and system requirements were achieved based on the applicable trust services criteria.

Sincerely,

Betsy Bevilacqua

Betsy Bevilacqua
VP, Information Security

ATTACHMENT A: Description of the Boundaries of the Reactor and KYT Systems

Company Overview

Chainalysis, Inc. (Chainalysis or Company or organization) is a blockchain analysis company that offers cryptocurrency compliance and investigative solutions to government agencies, exchanges, financial institutions, insurance, and cybersecurity companies. The Company was founded in 2014 and is privately owned. It has corporate headquarters in New York, New York with offices around the world supporting clients in more than fifty (50) countries. Chainalysis employs more than 500 employees worldwide. For more information, visit the Chainalysis website at www.chainalysis.com.

Chainalysis' software-as-a-service (SaaS) solutions maintain an aggregate mapping of cryptocurrency transactions to real world entities, defined as services and nodes operating cryptocurrency infrastructure. This information is programmatically embedded in existing workflows or visualized in the two market-facing SaaS solutions: Reactor and Know your Transaction (KYT).

Scope of the Report

Reactor and KYT

Reactor is a cryptocurrency investigation tool for tracing the flow of funds, which helps investigators as they identify and track bad actors who use cryptocurrencies for illicit activity. Reactor combines an intuitive interface with flexible visualization capabilities to map blockchain transactions into real-world entities, enabling users to combat criminal activity on the blockchain. Reactor is used every day by law enforcement, compliance officers, financial institutions, and governments around the world for criminal investigations.

KYT is an AML (anti-money laundering) compliance solution for monitoring cryptocurrency transactions, composed of real-time screening, case management, and enhanced due diligence. It automatically detects and alerts to patterns of potential high risk activity, from Office of Foreign Assets Control (OFAC) sanctioned addresses and darknet markets, to scams and anomalous transactions. KYT reduces manual workflows for cryptocurrency businesses by automating counterparty risk screening. KYT combines blockchain intelligence, an easy-to-use interface, and a real-time API to reduce manual workflows while helping cryptocurrency businesses comply with local and global regulations.

Components of the Reactor and KYT

Components of the Reactor and KYT

The purpose of the system description is to delineate the boundaries of the system, which include the services and commitments outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure

The Reactor and KYT infrastructure is hosted on Amazon Web Services (AWS). The resources are deployed inside AWS Virtual Private Cloud (VPC) within subnets and secured via security groups. The services are installed on Elastic Compute Cloud (EC2) instances and AWS container services (i.e. EKS). Additionally, Chainalysis utilizes Relational Database Service (RDS), for backend data processing and reporting for the in-scope systems, Simple Storage Service (S3) for backup storage. Access to the production systems for Chainalysis personnel is governed through OKTA SSO and multi-factor authentication is enabled for access to the AWS Console.

Software

Chainalysis is responsible for managing the development and operation of the Reactor and KYT systems including software development and maintenance of infrastructure components. The in-scope Chainalysis infrastructure and software components are shown in the table below:

Primary Software		
Software / Application	**Delivery Model**	**Purpose**
GitHub Enterprise Cloud	Cloud Hosted	Source Code Repository and Version Control
Jenkins	Cloud Hosted	Orchestration and deployment
Datadog	Cloud Hosted	Security event monitoring for infrastructure and cloud services
Humio	Cloud Hosted	Log aggregation, analysis, and storage
OKTA	Cloud Hosted	Authentication and identity access management (IAM)
Slack	Cloud Hosted	Internal communications
Jira	Cloud Hosted	Internal ticketing system
Zendesk	Cloud Hosted	Customer facing ticketing system
Jamf / Crowdstike	Cloud Hosted	Endpoint management

Data

Chainalysis applies advanced algorithms to publicly available observed transaction data. Data, as defined by Chainalysis, constitutes the following:

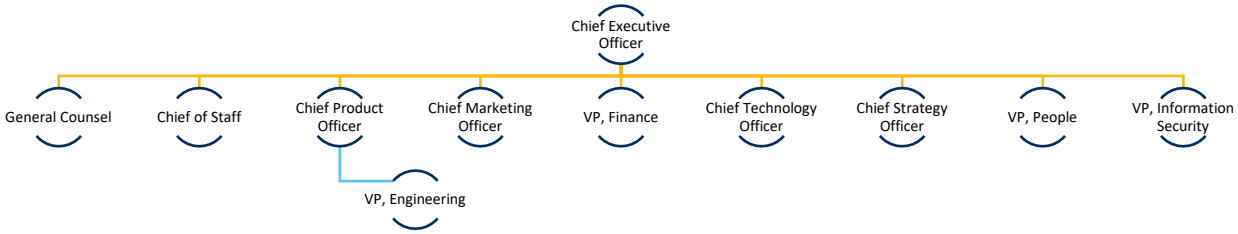
- Publicly available blockchain data:
  - Wallet Addresses
  - Sending Addresses
  - Receiving Addresses
  - Send Times
  - Receipt Times
  - Cryptocurrency Amounts
  - Transaction Hash
- Open Source Intelligence (OSINT)::
  - Chainalysis regularly scans publicly available websites for mentions of cryptocurrency addresses and transaction identities. This includes clear web and dark web sources, like forums and darknet markets.

People

Chainalysis organizational structure provides the overall framework for planning, directing and controlling operations. It utilizes an approach whereby personnel and business functions are segregated into departments according to job responsibilities, lines of reporting and communications, and allows employees to focus on the specific business issues impacting their customers. An organization chart is documented that clearly defines management authorities and reporting hierarchy. Below is a description of key Chainalysis' departments:

- Marketing: The marketing department is responsible for building the Company's brand, generating sales opportunities, and other marketing activities.
- Human Resources: The HR department is in charge of employee well-being and welfare. Additionally, HR also owns sourcing and recruitment operations.
- Client Support: The support team is responsible for providing support to Chainalysis' clients. The support team works closely with Operations, Product and Engineering departments to ensure that clients' needs are being met. They are responsible for submitting usability issues, and bugs. Client support is responsible for identifying and escalating client concerns and serves as L1 support.
- Legal: The primary responsibility of the legal team is to provide transactional support for Chainalysis business.
- Information Security: The Information Security department is responsible for the design, implementation, management, and review of Chainalysis' security policies, standards, baselines, procedures, and guidelines.
- Corporate IT: The Corporate Technology team at Chainalysis is responsible for the devices, infrastructure and services that employees rely on. It is an autonomous team dedicated to making sure that the teams at Chainalysis are empowered with hardware and software that they need to create the future of blockchain trust.
- Engineering: The Engineering department is responsible for developing, testing and validating Chainalysis' products and the business services implemented within the production environment.

Key internal corporate officers that are a part of the Executive Team include:



Policies and Procedures

Chainalysis has developed relevant policies, standards and procedures which are updated and approved annually by the ITS (Information Technology, TechOps, and Security) and respective Executive owners. These policies are made available to all Chainalysis employees through an internal Wiki. Additionally, Chainalysis' Privacy Policy is available on the organization's public website. Information Security standards include, but are not limited to:

- Overall Privacy and Security Governance
- Access Management Policy
- System Audits Logging and Monitoring
- Secure Software Development
- Security Policy Exception Management Process
- Disaster Recovery and Business Continuity Policy
- Data Classification Policy
- Event Logging Policy
- Baseline IT Security Best Practices for User Devices
- Information Security Incident Response Policy and Plan
- General Data Protection Regulation (GDPR) Policy
- Third Party Risk Management Policy
- Third Party Vendor and Security Policy Process
- Security Risk Management Policy
- Threat, Vulnerability and Patch Management Policy

Subservice Organizations

Chainalysis, Inc. (Chainalysis) uses a third-party service provider (subservice organization) to assist in the delivery of their Reactor and KYT products. Chainalysis has assumed that certain controls have been implemented by the subservice organization that are necessary, in combination with Chainalysis own controls, to provide reasonable assurance that Chainalysis service commitments and system requirements are achieved based on the applicable trust services criteria.

Below is a listing of the subservice organization used by Chainalysis, as well as the expected complementary subservice organization controls (CSOCs). Please refer to the description content within "Risk Assessment, Control Activities and Risk Mitigation" for activities performed by Chainalysis to monitor this subservice organization.

Subservice Organization	Services Provided	Expected CSOCs and Applicable Trust Services Criteria
Amazon Web Services (AWS)	● Infrastructure-as-a-Service (IaaS) cloud hosting services ● Data backup services	● AWS is responsible for implementing controls to manage logical access to the underlying network and virtualization management software for its cloud hosting services where Chainalysis systems reside. (CC6.2) ● Physical access to the applicable data centers hosting infrastructure is restricted to authorized personnel based on job responsibilities. (CC6.4) ● Physical access is monitored to detect unauthorized or inappropriate access. (CC6.4) ● Network protection procedures for the cloud environment through the use of a proprietary firewall and security monitoring applications that are configured and monitored by AWS personnel (CC7.2) ● Backup and disaster recovery procedures are in place (A1.3)

Complementary User Entity Controls

The Chainalysis Reactor and KYT control structure is designed with the assumption that certain controls would be implemented by user entities. This section describes user entity controls identified by Chainalysis as necessary to achieve certain applicable trust services criteria.

The user entity controls described below should not be regarded as a comprehensive list of all controls which should be employed by user entities. There may be additional controls that would be appropriate to address Security and Availability concerns which are not identified in this report. Each user entity is responsible for the identification, implementation and operation of appropriate controls to address their specific concerns as related to Chainalysis' Reactor and KYT.

Common Criteria 6: Logical and Physical Access

- User entities are responsible for the account administration for user administration within the application.
- User entities are responsible for notifying Chainalysis of changes made to technical or administrative contact information.
- User entities are responsible for providing Chainalysis with a list of approvers for security and system configuration changes for data transmission.
- User entities are responsible for protecting user logon information and user’s logon’s should be unique and not be shared.
- User entities are responsible for any network or internet connectivity required to access the Service over the Internet.

Common Criteria 7: System Operations

- User entities are responsible for immediately notifying Chainalysis of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers

Availability Criteria

- User entities are responsible for ensuring documented business continuity and disaster recovery plans are in place and tested for systems that interact with the Reactor and KYT systems.

ATTACHMENT B: Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Chainalysis has communicated the following principal service commitments to their clients relevant to the Security criteria of their Reactor and KYT systems:

Category	Communication Mechanism	Principal Service Commitments Network	Related System Requirements
Security	Master Service Agreement	• Implement reasonable security measures to protect customer systems and data, including enforcing access control, change control, and incident response. • Implement security procedures to safeguard against unauthorized access. • Encryption of data	• User access administration • Privileged access restrictions • Vulnerability Management • Information Technology Security Monitoring Alerts • External Application Penetration Testing • Data encrypted at rest • Data encrypted in transit
		• Notification of suspected security breach that affects customer data or system security.	• Internal security incidents are tracked and logged via a ticketing system. • Customer incidents are reported to the Customer Support Team, logged in respective tickets, and escalated if needed.
Availability	Master Service Agreement	• Processing capacity and usage requirements.	• Device logging and alerting
		• Disaster recovery capabilities	• Built-in redundancies and replication • Disaster recovery plan • Annual disaster recovery testing

Chainalysis has also identified control processes to help achieve their principal service commitments – the primary control processes for each commitment are summarized above as “Related System Requirements.”