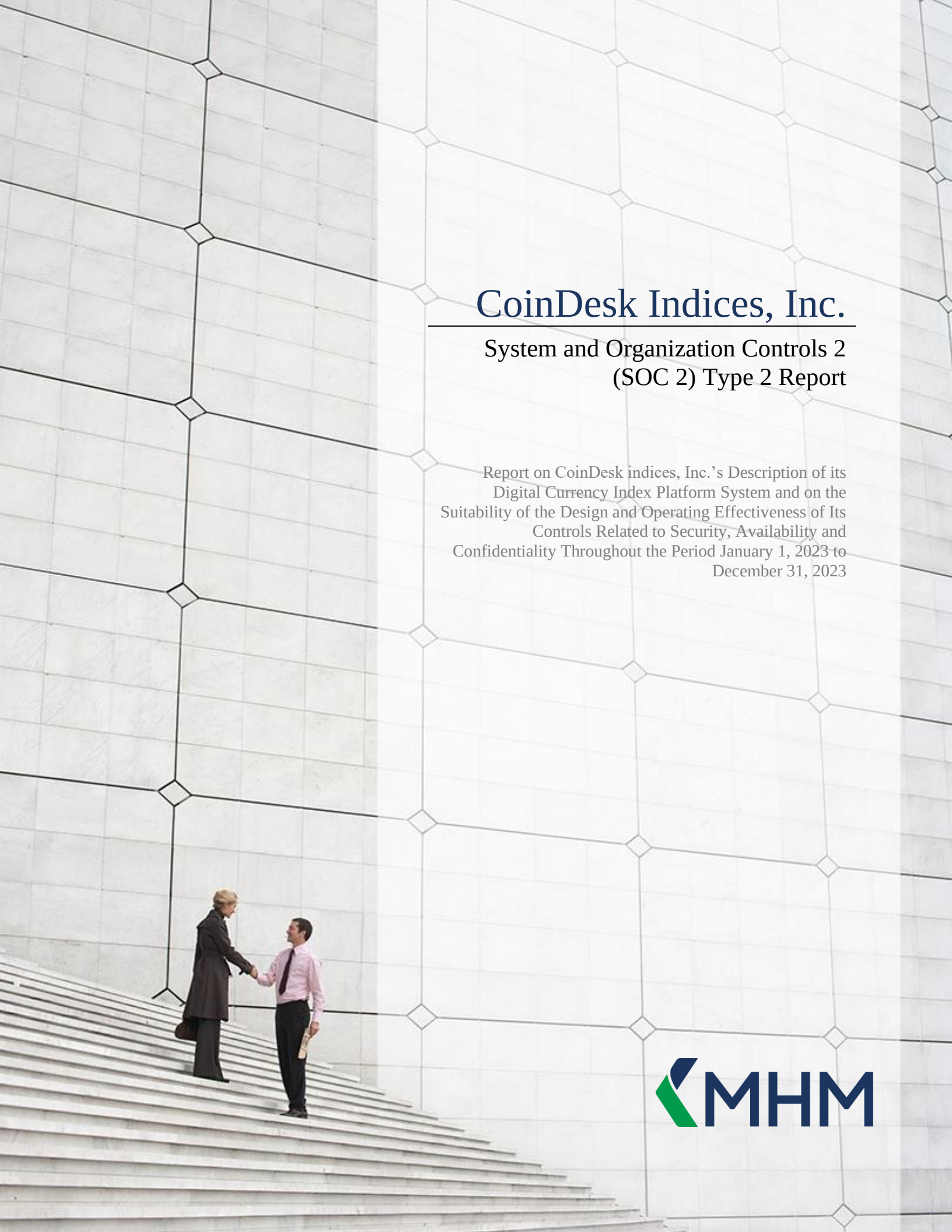


CoinDesk Indices, Inc.

System and Organization Controls 2 (SOC 2) Type 2 Report

Report on CoinDesk indices, Inc.'s Description of its Digital Currency Index Platform System and on the Suitability of the Design and Operating Effectiveness of Its Controls Related to Security, Availability and Confidentiality Throughout the Period January 1, 2023 to December 31, 2023

MHM

CoinDesk Indices, Inc.
SOC2 Report Relevant to Trust Services Criteria for Security, Availability, and Confidentiality
January 1, 2023 to December 31, 2023

TABLE OF CONTENTS

Section 1

Assertions of Management

Section 1 - Assertion of CoinDesk Indices, Inc.'s Management

We have prepared the accompanying description of CoinDesk Indices, Inc.'s system titled "CoinDesk Indices, Inc.'s Description of its Digital Currency Index Platform System" throughout the period January 1, 2023 to December 31, 2023 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Digital Currency Index Platform system that may be useful when assessing the risks arising from interactions with CoinDesk Indices, Inc.'s system, particularly information about system controls that CoinDesk Indices, Inc. has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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)*.

CoinDesk Indices, Inc. uses CoinDesk, Inc. to provide human resources and corporate information technology services. CoinDesk Indices, Inc.'s description includes a description of CoinDesk, Inc.'s human resources and corporate information technology services used by CoinDesk Indices, Inc. for user entities and business partners, including the controls of CoinDesk Indices, Inc. and the controls designed by CoinDesk Indices, Inc. and operated by CoinDesk, Inc. that are necessary for CoinDesk Indices, Inc. to achieve CoinDesk Indices, Inc.'s service commitments and system requirements based on the application trust services criteria. CoinDesk, Inc.'s assertion is presented on page 5 in section 1.

CoinDesk Indices, Inc. uses the following subservice organization: Amazon Web Services (AWS) for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CoinDesk Indices, Inc., to achieve CoinDesk Indices, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents CoinDesk Indices, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of CoinDesk Indices, Inc.'s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary; along with controls at CoinDesk Indices, Inc., to achieve CoinDesk Indices, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents CoinDesk Indices, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of CoinDesk Indices, Inc.'s controls.

We confirm to the best of our knowledge and belief that

a. the description presents CoinDesk Indices, Inc.'s System that was designed and implemented throughout the period January 1, 2023 to December 31, 2023, in accordance with the description criteria.

b. the controls stated in the description, including the controls designed by CoinDesk Indices, Inc. and operated by CoinDesk, Inc., were suitably designed throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that CoinDesk Indices, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization

and user entities applied the complementary controls assumed in the design of CoinDesk Indices, Inc.'s controls through that period.

c. the controls stated in the description, including the controls designed by CoinDesk Indices, Inc. and operated by CoinDesk, Inc., operated effectively throughout the period January 1, 2023 and December 31, 2023, to provide reasonable assurance that CoinDesk Indices, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization controls and complementary user entity controls assumed in the design of CoinDesk Indices, Inc.'s controls operated effectively throughout that period.

CoinDesk Indices, Inc.

Section 1 - Assertion of CoinDesk, Inc.'s Management

CoinDesk, Inc. provides human resources and corporate information technology services to CoinDesk Indices, Inc. The services provided by CoinDesk, Inc. are part of CoinDesk Indices, Inc.'s Digital Currency Index Platform system. We have prepared the portion of the accompanying description of CoinDesk Indices, Inc.'s Digital Currency Index Platform system titled "CoinDesk Indices, Inc.'s Description of its Digital Currency Index Platform System" throughout the period January 1, 2023 to December 31, 2023, (description) disclosing CoinDesk, Inc.'s human resources and corporate information technology services provided to CoinDesk Indices, Inc. based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about CoinDesk Indices, Inc.'s Digital Currency Index Platform system that may be useful, when assessing the risks arising from interactions with CoinDesk Indices, Inc.'s system, particularly information about system controls that CoinDesk Indices, Inc. designed, implemented and operated to provide reasonable assurance that is service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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*).

We confirm, to the best of our knowledge and belief, that

a) The description presents CoinDesk, Inc.'s human resources and corporate information technology services made available to CoinDesk Indices, Inc. throughout the period January 1, 2023 to December 31, 2023, in accordance with the description criteria.

b) CoinDesk, Inc.'s controls stated in the description, which were designed by CoinDesk Indices, Inc., operated as described throughout the period January 1, 2023 to December 31, 2023, based on the applicable trust services criteria.

CoinDesk, Inc.

Section 2

Independent Service Auditor's Report

Section 2 - Independent Service Auditor's Report

To: Management of CoinDesk Indices, Inc.

Scope

We have examined CoinDesk Indices, Inc.'s accompanying description of its Digital Currency Index Platform system, including human resources and corporate information technology provided services by and controls operated by CoinDesk, Inc. titled "CoinDesk Indices, Inc.'s Description of its Digital Currency Index Platform System" throughout the period January, 1, 2023 to December 31, 2023 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria) and the suitability of the design and operating effectiveness of CoinDesk Indices, Inc.'s controls, including the controls designed by CoinDesk Indices, Inc. and operated by CoinDesk, Inc. stated in the description throughout the period January, 1, 2023 to December 31, 2023, to provide reasonable assurance that CoinDesk Indices, Inc.'s service commitments and system requirements were achieved based on the trust service criteria relevant to security, availability, and confidentiality (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*).

CoinDesk, Inc. is an independent subservice organization providing human resources and corporate information technology services to CoinDesk Indices, Inc. The description includes those elements of the human resources and corporate information technology services provided to CoinDesk Indices, Inc. and the controls designed by CoinDesk Indices, Inc. and operated by CoinDesk, Inc. that are necessary for CoinDesk Indices, Inc. to achieve its service commitments and system requirements based on the application trust services criteria.

CoinDesk Indices, Inc. uses the following subservice organization: Amazon Web Services (AWS) for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CoinDesk Indices, Inc., to achieve CoinDesk Indices, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents CoinDesk Indices, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of CoinDesk Indices, Inc.'s controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at CoinDesk Indices, Inc., to achieve CoinDesk Indices, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents CoinDesk Indices, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of CoinDesk Indices, Inc.'s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Mayer Hoffman McCann P.C.
500 Boylston Street
Boston, MA 02116

Phone: 617.761.0600
Fax: 617.761.0601
mhmcpa.com

The information included in section 5, "Other Information Provided by CoinDesk Indices, Inc." is presented by CoinDesk Indices, Inc.'s management to provide additional information and is not part of the description. Information about CoinDesk Indices, Inc.'s response to identified exceptions has not been subjected to the procedures applied in the examination of the description and the suitability of the design of controls, and operating effectiveness of the controls to achieve CoinDesk Indices, Inc.'s service commitments and system requirements based on the applicable trust services criteria and, accordingly, we express no opinion on it.

Service Organization's Responsibilities

CoinDesk Indices, Inc. is responsible for its service commitments and system requirements and for designing, implementing and operating effective controls within the system to provide reasonable assurance that CoinDesk Indices, Inc.'s service commitments and system requirements were achieved. CoinDesk Indices, Inc. has provided the accompanying assertion titled "Assertion of CoinDesk Indices, Inc.'s Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. CoinDesk Indices, Inc. is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Subservice Organization's Responsibilities

CoinDesk, Inc. has provided the accompanying assertion titled "Assertion of CoinDesk, Inc. Management," (CoinDesk, Inc. Assertion) about the description and the controls stated therein. CoinDesk, Inc. is responsible for preparing the portion of the description related to the human resources and corporate information technology services provided to CoinDesk Indices, Inc. and the CoinDesk, Inc. assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; and implementing, operating, and documenting controls designed by CoinDesk Indices, Inc., which enable CoinDesk Indices, Inc. to achieve its service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design of and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively

- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

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

Inherent Limitations
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 individual users may consider important to meet their informational needs.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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 policies or procedures may deteriorate.

Description of Tests of Controls
The specific controls we tested and the nature, timing and results of those tests are presented in section 4.

Opinion
In our opinion, in all material respects

a. the description presents CoinDesk Indices, Inc.'s Digital Currency Index Platform system that was designed and implemented through the period January 1, 2023 to December 31, 2023, in accordance with the description criteria.

b. the controls stated in the description, including the controls designed by CoinDesk Indices, Inc. and operated by CoinDesk, Inc., were suitably designed throughout the period January, 1, 2023 to December 31, 2023 to provide reasonable assurance that CoinDesk Indices, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of CoinDesk Indices, Inc.'s controls throughout that period.

c. the controls stated in the description, including the controls designed by CoinDesk Indices, Inc. and operated by CoinDesk, Inc., operated effectively throughout the period January 1, 2023 to December 31, 2023 to provide reasonable assurance that CoinDesk Indices, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization and complementary user entity controls assumed in the design of CoinDesk Indices, Inc.'s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of CoinDesk Indices, Inc., user entities of the CoinDesk Indices, Inc.'s Digital Currency Index Platform system during some or all of the period January 1, 2023 to December 31, 2023, business partners of CoinDesk Indices, Inc. subject to risks arising from interactions with the Digital Currency Index Platform system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, 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, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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

Mayer Hoffman McCann P.C.

Boston, Massachusetts
April 3, 2024

Section 3

CoinDesk Indices, Inc.'s Description of its Digital Currency Index Platform System

Section 3 – CoinDesk Indices, Inc.'s Description of its Digital Currency Index Platform System

Overview of Operations

Company Background

CoinDesk Indices has three distinct product lines: single-asset reference indices, broad market and sector indices, and systematic strategy indices. The CoinDesk Bitcoin Price Index (XBX) has the longest index track record and underlies the world's largest digital asset products. The broad market and sector indices offer the most comprehensive broad market benchmarks, and the investible sectors are constructed using CoinDesk Indices' industry-adopted taxonomy. The systematic strategy indices help investors target specific outcomes.

In 2014, CoinDesk Indices launched with its flagship CoinDesk Bitcoin Price Index (XBX). Since then, financial institutions have been relying on the XBX and other CoinDesk Indices products to benchmark billions of dollars in assets under management.

CoinDesk Indices was acquired and established in 2021 as an independent subsidiary of CoinDesk, Inc., a trusted media platform for news and events for the next generation of investing and the future of money. With the acquisition, CoinDesk positioned itself to be a unified source for crypto media, events, research, pricing, and data. CoinDesk was an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups, until November 17, 2023, when CoinDesk was acquired by the Bullish group, owner of Bullish, a regulated, digital assets exchange. The Bullish group is majority-owned by Block.one. Both companies have interests in a variety of blockchain and digital asset businesses and significant holdings of digital assets, including Bitcoin.

The Digital Asset Classification Standard (DACS) was developed by CoinDesk Indices to provide a reliable, comprehensive, and standardized classification system for digital assets. Currently, the DACS includes the top 500 eligible digital assets by market capitalization and the DACS structure offers 3 levels of granularity across 7 Sectors, 26 Industry Groups and 40 Industries.

While DACS is unique to digital assets, it will serve many of the same functions as classification systems used for traditional asset classes. Among other things, DACS provides the market with a transparent and standardized method to determine sector and industry exposure, facilitates portfolio attribution analysis, and will help pinpoint investment opportunities.

Principal Service Commitments and System Requirements

CoinDesk Indices is committed to providing real-time indices and market data that is secure and available. The security approach revolves around the principle of "need to know" meaning that there is no access to information or systems that isn't explicitly allowed.

CoinDesk Indices establishes operational requirements that support the achievement of security, availability, and confidentiality commitments. Such requirements are committed in CoinDesk Indices' system policies, procedures, and client contracts. Information security and compliance policies define an organization-wide approach to how systems and data are protected. In addition to these policies, standard operating procedures have been documented on how to carry out specific processes required in the operation and development of CoinDesk Indices and market data.

Components of the System Used to provide the Service

Boundaries of the System

The scope of this SOC 2 is solely around the Digital Currency Index Platform system (the "System") that maintains CoinDesk Indices and market data as operated and managed by the team during the period under review. The scope does not include other CoinDesk, Inc. services and offerings.

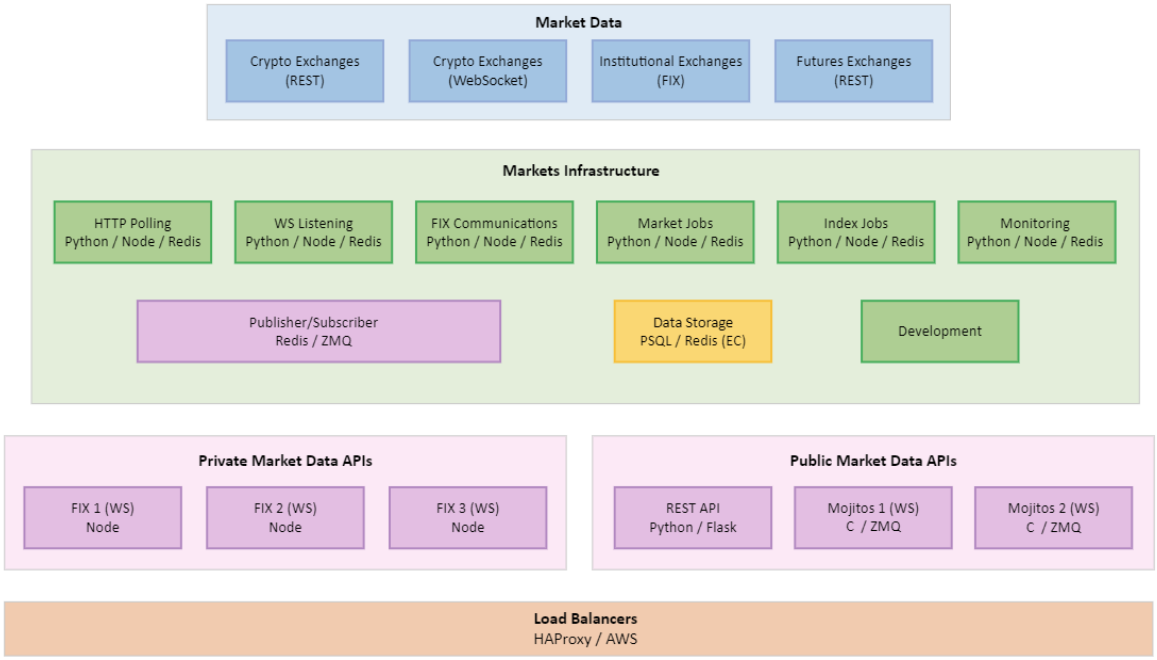
Infrastructure

Supporting servers for market data are responsible for collecting trade data from exchanges, calculating index and reference rate values, building candles, sending data directly to client emails, publishing data to WebSocket, REST API, and archiving data.

Indices and market APIs (Application Programming Interface) provide programmatic access to normalized data from market venues and for CoinDesk Indices' proprietary indices. The API is designed for low-latency, high-throughput applications that require high availability.

The System is 100% hosted in AWS. The System functionality depends on the following AWS and ancillary services:

- AWS Elastic Container Registry (ECR) - Serverless Computation and Containerization
- AWS Fargate - Serverless Computation and Containerization
- AWS Lambda - Serverless Computation and Containerization
- Elastic Compute Cloud (EC2) - Application hosting – Market boxes
- Identity Access Management (IAM) – Access control
- GitHub – Development and version control
- Load Balancer – Reverse proxy and traffic distributor
- Mojitos - WebSocket
- MongoDB – Database storage
- RabbitMQ – Calculation logs
- Redis – Database, cache, message broker
- Relational Database Service (RDS) – Postgre SQL database
- Simple Storage Service (S3) - Digital asset/file storage
- Squid-proxy – Proxy for exchange integration



Software

CoinDesk Indices is supported by systems and software used for the delivery of indices and market data and services, which include:

- AWS Inspector – Vulnerability Management
- AWS GuardDuty – Threat Detection
- BambooHR – Human Resource documentation and personnel management
- Confluence – Team collaboration and policy retention
- Grafana – Observability monitoring
- Jira – Change management, user provisioning and workflows
- PagerDuty – System and Application Alerting
- Sophos Intercept X Advanced – Anti-malware protection and detection
- Terraform - Infrastructure as code
- WireGuard – Remote access and virtual private network (VPN)

People

CoinDesk Indices personnel involved in the operation, success, and use of the System are:

- Executive Management
    - President
        - Responsible for general oversight of business operations and the culture of the organization.
    - Head of Index Governance and Operations

        - Responsible for day-to-day production and oversight of the indices and governance of new products or changes to existing products.
    - Head of Engineering
        - Responsible for development and day-to-day operations of the System
    - Product Owner
        - Responsible for product development with regards to the System.

- Information Security Committee
    - Provide guidance, oversight, and direction to CoinDesk Indices' teams as it relates to data governance, privacy, compliance, and information security initiatives undertaken by the organization. The Committee includes at least one member who is not involved in the performance of controls.

- Security, Risk, and Compliance Team
    - Oversee and monitor the security and compliance of systems and assets utilized to support the System.

- Engineering Team
    - Developers
        - Write and maintain code for the frontend and backend of the System, such as new features, patches, and bug fixes.
    - Site Reliability Engineers
        - Responsible for the infrastructure that hosts and supports the System. Supports information technology, security, and compliance responsibilities.

- Product Management Team
    - Research and identify opportunities to create new product functionality and indices.
    - Responsible for collecting and organizing feedback and enhancement requests from current clients.
    - Responsible for revenue-generating activities. This includes managing digital marketing initiatives, the creation and maintenance of digital marketing assets and all sales and renewal activity.

Procedures

The Information Security Committee and supporting management personnel maintain and annually review the following documented CoinDesk Indices operating policies and procedures:

- Acceptable Use of Technology
- Business Continuity Management (BC) Policy; Plan
- Change Management Policy; Procedures
- Client Account Management Procedures
- Code of Conduct

- Confidentiality and Rights Agreement
- Conflict of Interest Policy
- Cybersecurity Policy
- Data Classification and Handling Policy
- Disaster Recovery (DR) Policy; Plan
- Employee Handbook
- Incident Response (IR) Plan
- Pandemic Policy
- Password Standards Policy
- Remote Access Policy
- Provisioning Procedures
- Risk Management Policy
- Vendor Management Policy
- Whistleblowing Policy

1. Physical Security

The System is hosted entirely on AWS so all physical security relating to the infrastructure is provided by Amazon.

2. Logical Security

Employee Authentication and Authorization

Authentication requirements (password configuration settings and multifactor authentication) to the System's backend environment are configured in accordance with CoinDesk Indices' Password Standards Policy. Employee access to the backend environment is restricted to only appropriate and documented personnel that require access to perform their job responsibilities.

CoinDesk Indices also deploys authentication requirements (password configuration settings and multifactor authentication) for software, tools, and other solutions used to support the operation of the System. Authentication requirements to access client information, the source code repositories and deployment tools are configured in accordance with CoinDesk Indices' Password Standards Policy. Furthermore, access is restricted to authorized personnel that require access to work with the source code or migrate code to different environments.

Access Provisioning

New access to in-scope components must be approved by authorized Management, documented, and follow a predefined workflow. The requestor and reason for the new access is also documented within an Onboarding or Change of Access ticket. Evidence of approval or denial, who approved it and when, is retained within the request ticket.

On at least an annual basis, accounts that support the systems and software used for the delivery of indices and market data services are reviewed. If an account is determined to not be required, it is removed and documented in the dedicated ticket workflow.

Access Removal

Terminated employees' access to in-scope systems is removed in a timely and expedited manner per CoinDesk Indices' defined workflow. Access to systems, applications, and accounts are documented and retained through an employee's tenure at the organization. Upon termination, remote access to the System is removed. Depending on the type of access, the responsible party is assigned for removing access to that account from the terminated employee. Each of these accounts has a manager and backup listed. Depending on the type of account, this would involve a password change or removing the employee's user from the account. If required, user access to accounts that involve a password change and maintain being active beyond termination are documented.

Privileged Access

Administrative privileges to AWS and supporting systems are limited to only authorized and documented personnel. Access administrative activity, including but not limited to system changes, adding new assets, and adding new users in the production environment is logged and monitored.

On a quarterly basis, accounts with privileged accounts to in-scope services and resources are reviewed by the Information Security Committee. If an account is determined to not be required, it is removed and documented in the dedicated ticket workflow. Compliance ensures that privileged access to all in-scope services and resources are at least reviewed annually.

Users with heightened system access, attend technical security training to ensure they are up to date on cyber vulnerabilities and threats.

3. Network Security

The Information Security Committee maintains an inventory of company IT assets, including AWS applications and resources. Management has documented network diagrams detailing AWS applications, data pathways and data participants. Diagrams are reviewed annually and updated as necessary.

Secured and encrypted connections are required for external devices connecting to client information, code repositories, and AWS environment and internal services. Information transmitted over public networks is encrypted during transit.

Network policy rules have been established for controlling traffic in and out for externally facing assets within AWS.

A key management system is utilized to create and manage encryption keys. These keys are created and managed within AWS Key Management Service. Keys are rotated on an annual basis.

Monitoring and analytics for anomalies, potential security breaches, and adherence to company best practices is used to support the security and efficiency of the System. From 1/1/2023 through 6/30/2023, system logs were collected and analyzed by the Security team on a biweekly basis for possible or actual attempts to breach the network. Identification of anomalies or issues are reviewed by the Engineering Team

to validate the legitimacy. True anomalies and issues are documented, and remediation is tracked to resolution.

As of 7/1/2023, CDI implemented a Log Management and Threat Analytic system to ingests log data from AWS resources and services and compares the activity against third-party threat intelligence data. Suspicious activity is noted on daily summaries and real-time alerts sent to the Information Security team. Alerts are reviewed and addressed as soon as possible, as needed.

4. Change Management

Application Change Management

CoinDesk Indices has a formal systems development life cycle (SDLC) methodology that governs the development, implementation, and maintenance of information systems and related technology requirements.

The Engineering Team employs an Agile project methodology, specifically Scrum, for production fixes and enhancements. Production fixes are done by dedicated developers. The development team is composed of Vice President of Engineering and backend engineers. Additionally, oversight is provided by executive management and the product owner. Meetings are held using a bi-weekly sprint cadence.

At the beginning of each sprint, the sprint planning meeting is held. The attendees include all developers, the Head of Engineering, and Product Owners. Product Owners explain each product request in detail, the developers estimate the effort required to complete the item, which includes development, testing, and deployment to production. If approved for the sprint, the item is then moved into a sprint. This is done for each backlog item until we exceed the average effort per sprint.

The sprint review meeting is held at the end of each sprint. During this meeting, Engineering Team members provide the demo of the system integration (SI) that he/she has worked on, and feedback is provided by others. Any follow-up action items are documented and added to the next sprint.

In the event of an identified emergency change, the lifecycle of the change will be executed with utmost urgency. There may be fewer people involved in the change management process review, and the change assessment may involve fewer steps, but any emergency change must still be authorized by the management team, even in cases where the change is not reviewed in advance. Emergency changes are recorded and retained in the change log.

Changes to the System are documented in the change log, authorized, tested, and approved prior to migration to production. Changes to system code are developed and tested in separate development and staging environments before implementation. The change log is handled by our project management software, Jira.

Infrastructure and Network Change Management

AWS infrastructure changes are documented and tracked throughout the entirety of the change process. All changes to the AWS infrastructure are recorded within weekly meetings held during the change lifecycle

to discuss pending questions, blockers, and the progress of the change. All changes must be reviewed prior to implementation into the production environment.

The above change process is applied to all servers and services that are critical to the production environment's availability and functionality.

All changes impacting the security of ancillary systems that contain client information or support systems and software used for the delivery of indices and market data are tracked within a dedicated security change log and follow the standards within the Change Management Policy.

If it is decided that the change shall be tested, changes are made to an AWS virtual private cloud (VPC) development environment first and tested until the team is confident that the change can be pushed to the staging and finally production environments.

5. Vulnerability Management

Anti-virus and endpoint vulnerability detection software is installed on all user endpoints. Nightly scans are performed to ensure no vulnerabilities exist, and virus definitions are updated daily.

Infrastructure as code is utilized for changes made to the production environment. Amazon Machine Images (AMI) are a parameter of CoinDesk Indices EC2 instances which are managed and configured via Terraform. In the event parameters are changed to an instance, an alert is generated and sent to the Information Security team.

Systems within AWS are defined and set-up with pre-configured Ansible playbooks. Dedicated playbooks include system security hardening standards which are applied across all systems.

CoinDesk Indices performs quarterly vulnerability assessments on all running EC2 instances through the use of AWS and enterprise-identified tools. Results are reviewed by the Information Security Committee and prioritized for remediation. Any vulnerabilities with critical or severe severity level are prioritized and remediated within a defined period.

6. Incident Management

Once the CoinDesk Indices Incident Response Coordinator declares an incident, the Incident Response Plan is invoked which details the roles and responsibilities, process and decisions to be made going forward.

A standardized incident response form is made available to authorized employees and utilized for documenting information through the lifecycle of an incident. Incidents are categorized by severity and type of incident which could include but not limited to the following:

- System Interruption/Outage
- Programming Error
- Malicious Code
- Denial of Service

- Phishing/Social Engineering
- Unauthorized Access
- Loss of Data
- Third-party Incident
- Criminal Activity

7. Data Management

Data in Transit

All data transmitted externally over public networks to clients from the System is encrypted using Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS) 1.2.

Data at Rest

CoinDesk Indices' clients are not granted access to internal systems and do not have access to other client's data. Indices and market data are made available outbound from the System via API.

Amazon S3 Infrastructure as a Service (IaaS) is natively encrypted within AWS.

Data Destruction

Unless otherwise agreed upon, CoinDesk Indices will delete client data no longer than 30 days after a client has terminated their account. The execution of this task is documented and tracked in a change log system.

Standards have been documented for the disposal of confidential data and assets containing confidential data. Evidence of the disposal or destruction is documented and retained.

8. Backups and Recovery

Backup Strategy

Back-ups are scheduled and retained for all critical Production resources in accordance with procedures. All critical production resources are backed up nightly. Production backups are copied in two different AWS geographic regions for redundancy; US-West-2 and a disaster recovery vault in US-East-1. In the event a backup fails, an alert is sent to the Site Reliability Engineer team for investigation and remediation.

Testing is performed on a scheduled on a quarterly basis to validate backups are reliable and data is recoverable. The test is performed annually, and documented and retained within a dedicated change management ticket.

CoinDesk Indices deploys critical AWS resources and services (databases, digital assets, and web servers) to multiple data centers in AWS' US-West-2 region (Oregon) physically secured by AWS to ensure physical redundancy.

Disaster Recovery Testing

CoinDesk Indices has a disaster recovery (DR) plan which it reviews on a periodic basis for completeness and accuracy. On an annual basis, CoinDesk Indices employees participate in a disaster recovery exercise

which is designed to evaluate the efficiency of processes for recovering and restoring data and/or business systems. Changes to the DR plan are documented, recorded within a dedicated change management ticket, and tracked to resolution.

9. Availability

System Availability

Baseline rate limits have been defined on CDI's load balancers to ensure traffic to the CDI services is managed and available for all authorized customers.

Indices and market data is hosted on redundant production servers (one primary and two replicas) and where possible, resources are deployed redundantly across multiple availability zones to ensure durability and redundancy.

System health and availability are monitored through an enterprise monitoring system. Alarm criteria are established and managed by Site Reliability Engineers, and management. These include the reachability of the services hosted as well as underlying system metrics such as Central Processing Unit (CPU) usage, disk storage, and memory utilization. Triggered alarms are sent to Site Reliability Engineers for investigation and resolution.

Capacity and performance forecasting is performed on an ongoing basis to evaluate system demands. Resources are allocated where necessary. The change management process is initiated when system usage exceeds control tolerances. Tolerances are defined based on the resource requirements for each system component and set at a level to allow for changes to be made proactively. Alerts are generated when defined tolerances are met and/or exceeded.

10. Confidentiality

Internally, confidentiality requirements are communicated to employees through training and policies. Employees are required to attend annual security training, which includes topics related to protecting a client's content. Confidentiality requirements are included in the Data Classification and Handling Policy. Policies are reviewed and updated as needed, or at minimum annually by the Information Security Committee.

During CoinDesk Indices system and software design, build, and test of product features, client data is not utilized. Client data is not required for the CoinDesk Indices software development life cycle. When content is required for the development or test of a service's software, engineering teams utilize mock or random data.

CoinDesk Indices implements controls to restrict and monitor access to resources that process or store client content. Access to client data is restricted to only employees with an authorized business need. In addition, Confidentiality and Rights Agreement (CRA) binds an employee and subcontractor to confidentiality in the unlikely event they are exposed to client information.

Services and systems hosted and managed by CoinDesk Indices are designed to retain and protect a client's information for the duration of the client agreement period, and in some cases, up to 30 days beyond termination.

Additionally, CoinDesk Indices retains client content per Master Licenses Agreement.

Data

Client and Company data are protected through technical, administrative, and physical controls covered in the Procedures section of this report. Data maintained by CoinDesk Indices is defined into three categories, Confidential, Private, and Public. The production environment is designed to only maintain internal company-related proprietary information. Confidential client personally identifiable information (PII) is not utilized or retained within production systems and is limited to ancillary systems, such as the company's customer relationship management (CRM) tool.

Subservice Organizations

Amazon Web Services (AWS) provides the infrastructure as a service (IaaS) solution. Every layer of the System from development to hosting is hosted in AWS. That being the case, AWS is solely responsible for the physical security of the infrastructure the System is hosted on. Most of AWS's services offer some degree of redundancy and resiliency out of the box but being able to integrate across servers and data centers allows the System to expand on that.

CoinDesk, Inc. provides human resources and corporate information technology, marketing, and finance services, as the parent company of CoinDesk Indices. CoinDesk employees are restricted from having access to production systems that support indices and market data. If access to any ancillary systems is required, employees are provisioned with a CoinDesk Indices device and account. CoinDesk employees are required to sign a Confidentiality and Rights Agreement, the Acceptable Use of Technology Policy, and abide by processes set forth by CoinDesk Indices.

Subservice Organizations Monitoring

AWS status is monitored using their public-facing Service Health Dashboard at https://status.aws.amazon.com/. The vendor, and associated SOC 2 report, is reviewed on an annual basis.

CoinDesk Indices periodically audits and investigates the systems managed by CoinDesk, Inc. to ensure access is provisioned correctly and system controls meet a defined standard.

Sprint reviews at the end of each sprint provides insight into what is done and what is left. Continuous testing of the application provides the quality of the application.

Control Environment

Governance

CoinDesk Indices has established an Employee Handbook and Code of Conduct which outlines the organization's commitment to integrity and ethical values and their expectations regarding employee

conduct. All newly hired employees must read the Handbook, Code of Conduct, and provide a signed acknowledgement.

Human Resources

Background checks are performed for employees who have access to corporate resources or customer data as a contingency of employment and to ensure there are no conflicts with CoinDesk Indices values. Further, all new CoinDesk Indices employees are required to sign a Confidentiality and Rights Agreement as well as sign the Acceptable Use of Technology Policy and data protection policies.

Performance reviews are conducted on an annual basis by the employee's supervisor and results are submitted to Human Resources. Employee performance and adherence with Corporate Values and Ethics goals are covered.

Roles and Responsibilities

Job descriptions are documented that outline roles and responsibilities for all active positions. Further, CoinDesk Indices has an organizational chart formally documenting the chain of command and authorities.

Risk Assessment

CoinDesk Indices designated Information Security Committee member performs a risk assessment annually using an industry-standard risk management framework which includes:

a. Evaluating the effect of regulatory, technological, and environmental changes on CoinDesk Indices system security.

b. Involving appropriate levels of management.

c. Analyzing risks associated with the threats.

d. Identifying threats to operations, including security threats.

e. Identifying threats to operations, including threats from vendors, business partners, and other parties.

f. Considering changes that could significantly impact CoinDesk Indices system of internal control.

g. Determining a risk mitigation strategy and remediation tracking mechanism.

h. Communicating annual risk assessment results and risk mitigation strategy to the Information Security Committee.

New vendors and business partners are required to go through an information security assessment. Depending on the type of services and access to confidential information, an annual risk assessment is conducted by the Information Security Committee. Assessment results and approval are documented in CoinDesk Indices vendor management tool.

Risk Mitigation

CoinDesk Indices has a formal remediation tracking system to ensure IT and Security issues detected from internal processes or external audits/reviews are centrally recorded, responded to, and tracked to resolution.

Trust Services Criteria and Related Control Activities

Management selects, implements and manages control activities through Policies and Procedures. Refer to the above Procedures section for the Company's relevant control activities.

Trust Services Criteria Not Applicable to the In-Scope System

CC6.4 is not applicable to the System as all aspects are hosted in the Amazon Web Services System and CoinDesk Indices personnel work remotely. As such the below criteria was not assessed:

> *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.*

Information and Communication

Internal Communications

Internal communications to employees and staff are managed through two different channels, Slack and Confluence. Updates impacting the System and associated applications are provided via predefined Slack channels. In addition, policies, procedures, and other company resources are made available to employees and staff within a dedicated Confluence page.

External Communications

Defined standards have been established for communicating incidents, failures, concerns, and other matters with external parties. In the event of an incident, system failure, or control change that affects external clients or stakeholders' communication is sent out to explain the problem and when they can expect a resolution. Further, Master License Agreements are established with external parties to provide the responsibilities, boundaries, confidentiality, and service levels to set expectations.

Monitoring Activities

Ongoing Monitoring

An inventory of key security controls implemented is formally maintained. On an annual basis, the Information Security Committee and control owners review, approve and if needed, modify the control wording. Controls are reviewed throughout the year in accordance with a defined internal audit schedule that is approved by the Information Security Committee. The audit program is broken down into quarterly audits with dedicated testing requirements. Findings noted via the audit cycle are documented and tracked to resolution.

All employees are required to participate in an annual and monthly Security and Privacy training. Additionally, employees and contractors are required to review and acknowledge corporate policies and procedures upon hire and on an annual basis.

The Security and Compliance team and Site Reliability Engineers are automatically alerted anytime deployment to production is performed. If deployment activity was not expected, they investigate the change to determine it was authorized.

Complementary Subservice Organization Controls

The Company relies on following services and complementary controls at the subservice organizations as part of its controls in meeting the following trust services criteria:

TSP Ref #	Applicable Subservice Organization	Complementary Subservice Organization Controls
CC6.1, CC6.4, CC7.1, CC7.2, CC8.1, A1.1, A1.2	AWS	AWS is responsible for logical access, change management, and computer operations controls related to the hosted infrastructure and physical security and environmental control around its data centers.
CC1.1, CC1.4, CC1.5	CoinDesk	CoinDesk, Inc. is responsible for controls related to human resources and corporate information technology services.

Section 4

Trust Services Category, Criteria, Related Controls and Tests of Controls

Section 4 - Trust Services Category, Criteria, Related Controls and Tests of Controls

TESTS OF OPERATING EFFECTIVENESS

Our tests of the operational effectiveness of controls were designed to cover a representative number of transactions throughout the period of January 1, 2023 to December 31, 2023, for each of the controls listed in this section, which are designed to meet the applicable trust services criteria. In selecting particular tests for the operational effectiveness of controls, we considered (a) the nature of the items being tested, (b) the types of available evidential matter, (c) the nature of the audit objectives to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test.

Test	Description
Inquiry	Made inquiries of appropriate personnel and corroborated responses with management.
Observation	Observed application or existence of specific controls.
Inspection	Inspected documents and reports indicating performance of the control.

PROCEDURES FOR ASSESSING COMPLETENESS and ACCURACY OF INFORMATION PROVIDED BY THE ENTITY (IPE)

For tests of controls requiring the use of IPE (e.g., controls requiring system-generated populations for sample based testing), we perform a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspect the source of the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) tie data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity. In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), we inspect management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

TSP Ref #	Trust Services Criteria	Management Control Activity Reference
SECURITY (COMMON CRITERIA)		
CC1.1 - Control Environment	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	CDI-1.1.2, CDI-1.2.1
CC1.2 - Control Environment	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	CDI-1.1.1, CDI-1.2.1
CC1.3 - Control Environment	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	CDI-1.1.1, CDI-1.2.1, CDI-1.3.1, CDI-2.1.1
CC1.4 - Control Environment	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CDI-1.1.2, CDI-1.1.3, CDI-1.4.1
CC1.5 - Control Environment	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CDI-1.2.1, CDI-1.4.1
CC2.1 - Communication and Information	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CDI-1.1.1, CDI-1.4.2
CC2.2 - Communication and Information	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	CDI-1.1.2, CDI-1.2.1, CDI-1.3.1, CDI-1.4.2
CC2.3 - Communication and Information	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	CDI-2.2.1, CDI-2.2.2
CC3.1 - Risk Assessment - Operations Objectives	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CDI-1.1.1, CDI-1.1.2, CDI-1.2.1, CDI-1.3.1, CDI-1.4.2, CDI-2.2.2, CDI-3.1.1, CDI-4.1.1

TSP Ref #	Trust Services Criteria	Management Control Activity Reference
CC3.2 - Risk Assessment	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.	CDI-1.1.3, CDI-1.2.1, CDI-3.1.1, CDI-3.1.2, CDI-4.1.1, CDI-6.8.1, CDI-7.1.2, CDI-7.2.1, CDI-7.3.1, CDI-A1.1.1
CC3.3 - Fraud Risk Assessment	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CDI-1.1.2, CDI-1.1.3, CDI-1.2.1, CDI-3.1.1, CDI-4.1.1
CC3.4 - Assessing Changes in Risk	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	CDI-1.2.1, CDI-2.2.2, CDI-3.1.1, CDI-3.1.2, CDI-4.1.1, CDI-7.1.2, CDI-A1.3.2
CC4.1 - Monitoring Activities - Periodic Evaluations	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.	CDI-4.1.1, CDI-7.1.2
CC4.2 - Monitoring Activities - Exception Monitoring	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.	CDI-4.1.1, CDI-7.1.2
CC5.1 - Control Activities - Risk Mitigation	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.	CDI-1.1.1, CDI-1.1.2, CDI-1.2.1, CDI-3.1.1, CDI-4.1.1
CC5.2 - Control Activities - IT General Controls	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	CDI-1.1.1, CDI-1.1.2
CC5.3 - Control Activities - Polices / Procedures	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	CDI-1.1.1, CDI-1.1.2, CDI-1.2.1, CDI-2.1.1, CDI-2.2.1, CDI-4.1.1
CC6.1 - Logical and Physical Access Controls	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.	CDI-6.1.1, CDI-6.1.2, CDI-6.1.3, CDI-6.1.4, CDI-8.1.5

TSP Ref #	Trust Services Criteria	Management Control Activity Reference
CC6.2 - Logical and Physical Access Controls - User Provisioning	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.	CDI-6.1.2, CDI-6.1.3, CDI-6.2.1, CDI-6.2.2, CDI-6.3.1
CC6.3 - Logical and Physical Access Controls - User Provisioning	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.	CDI-6.1.2, CDI-6.1.3, CDI-6.2.1, CDI-6.2.2, CDI-6.3.1
CC6.4 - Logical and Physical Access Controls - Physical Access	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.	All information systems are hosted by third parties and those third parties are responsible for physical access to the data center facilities
CC6.5 - Logical and Physical Access Controls - Data Destruction	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.	CDI-1.1.1, CDI-6.3.1, CDI-6.5.1, CDI-6.5.2
CC6.6 - Logical and Physical Access Controls - User Authentication	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CDI-6.1.2, CDI-6.7.2
CC6.7 - Logical and Physical Access Controls - Data In-Transit	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.	CDI-6.2.1, CDI-6.3.1, CDI-6.7.1, CDI-6.7.2, CDI-6.7.3, CDI-7.1.1
CC6.8 - Logical and Physical Access Controls - Unauthorized / Malicious Software	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	CDI-6.8.1, CDI-7.1.2, CDI-7.2.1, CDI-8.1.4

TSP Ref #	Trust Services Criteria	Management Control Activity Reference
CC7.1 - System Operations - Configuration Standards	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.	CDI-5.1.1, CDI-7.1.1, CDI-7.1.2, CDI-7.2.1
CC7.2 - System Operations - Security Events	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.	CDI-1.1.1, CDI-7.2.1
CC7.3 - System Operations - Security Incidents	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.	CDI-7.2.1, CDI-7.3.1
CC7.4 - System Operations - Incident Response	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	CDI-2.2.1, CDI-2.2.2, CDI-7.3.1
CC7.5 - System Operations - Incident Recovery	The entity identifies, develops, and implements activities to recover from identified security incidents.	CDI-2.2.2, CDI-7.3.1, CDI-A1.3.1
CC8.1 - Change Management	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CDI-1.1.1, CDI-1.1.2, CDI-4.1.1, CDI-6.1.3, CDI-8.1.1, CDI-8.1.2, CDI-8.1.3, CDI-8.1.4, CDI-8.1.5
CC9.1 - Risk Mitigation	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CDI-2.2.2, CDI-3.1.2
CC9.2 - Third Party Risk Management	The entity assesses and manages risks associated with vendors and business partners.	CDI-2.2.2, CDI-3.1.2

TSP Ref #	Trust Services Criteria	Management Control Activity Reference
AVAILABILITY		
A1.1 - Data Capacity Planning / Monitoring	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.	CDI-A1.1.1, CDI-A1.1.2
A1.2 - Environmental Control / Back-ups	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.	CDI-A1.2.1, CDI-A1.2.2
A1.3 - Data Recovery	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	CDI-A1.3.1, CDI-A1.3.2
CONFIDENTIALITY		
C1.1 - Identify / Maintain Confidential Information	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	CDI-1.1.1, CDI-1.4.2, CDI-2.2.2, CDI-6.5.2
C1.2 - Data Disposal	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	CDI-1.1.1, CDI-1.1.2, CDI-1.1.3, CDI-6.2.1, CDI-6.5.1, CDI-6.5.2

Service Organization Control Activities:

Below represents the key control activities identified by CoinDesk Indices, Inc. to meet the Security, Availability, and Confidentiality Trust Services Criteria, and the related Auditor testing procedures and results.

Management Control Activity	Test Procedures Performed by MHM	Results of Tests
SECURITY (COMMON CONTROLS)		
CDI-1.1.1: CoinDesk Indices maintains documented policies and procedures that provide oversight and guidance as it relates to Information Technology and Security within the organization.	Inspected Corporate IT and Security policies and procedures to determine that CoinDesk Indices maintains documented policies and procedures that provide oversight and guidance as it relates to Information Technology and Security within the organization.	No Exceptions Noted
CDI-1.1.2: Employees and contractors are required to review and acknowledge corporate policies and procedures upon hire. Policies and procedures are made available to all employees across the organizations.	For a sample of new employees and contractors, inspected their initial sign off of corporate policies and procedures to determine employees and contractors are required to review and acknowledge corporate policies and procedures upon hire. Observed CDI's confluence page to determine that policies and procedures are made available to all employees across the organizations.	No Exceptions Noted
CDI-1.1.3: A national-wide background check is performed on all new CoinDesk Indices employees who have access to corporate resources or customer data.	For a sample of new employees, inspected their completed background check to determine CoinDesk Indices Employees who have access to corporate resources or customer data will have a background check performed according to the corporate standards.	No Exceptions Noted
CDI-1.2.1: CoinDesk Indices has an Information Security Committee that exercises oversight of the development and performance of internal controls. The Committee includes at least one member who is not involved in the performance of controls and formally meets monthly.	Inspected the Information Security Committee Charter and a sample of monthly committee meeting minutes to determine that CoinDesk Indices has an Information Security Committee that exercises oversight of the development and performance of internal controls and formally meets monthly. Inspected the listing of members in the Information Security Committee charter and CDI Organizational chart to determine that the Committee includes at least one member who is not involved in the performance of controls.	No Exceptions Noted

Management Control Activity	Test Procedures Performed by MHM	Results of Tests
CDI-1.3.1: CoinDesk Indices has defined structures, reporting lines with assigned responsibilities to appropriately meet requirements relevant to security, availability, and confidentiality.	Inspected the CDI organizational chart and job descriptions for a sample of current employees to determine that CoinDesk Indices has defined structures, reporting lines with assigned responsibilities to appropriately meet requirements relevant to security, availability, and confidentiality.	No Exceptions Noted
CDI-1.4.1: CoinDesk Indices performs an annual employee evaluation of staffing and assignments. Employees receive feedback from management on areas of strength and growth opportunities.	For a sample of employees, inspected their completed annual employee evaluation and sign off from their supervisor to determine that CoinDesk Indices performs an annual employee evaluation of staffing and assignments and employees receive feedback from management on areas of strength and growth opportunities.	No Exceptions Noted
CDI-1.4.2: CoinDesk Indices conducts periodic training to educate and promote security awareness and requirements that are in alignment with corporate policies.	For a sample of current employees and security awareness training events, inspected the periodic security awareness training attendance records to determine that CoinDesk Indices conducts periodic training to educate and promote security awareness and requirements that are in alignment with corporate policies.	No Exceptions Noted
CDI-2.1.1: Corporate policies are reviewed and approved on an annual basis by the Information Security Committee (ISC).	Inspected the ISC approval on policies and procedures to determine that Corporate policies are reviewed and approved on an annual basis by the Information Security Committee (ISC).	No Exceptions Noted
CDI-2.2.1: CoinDesk Indices has established standards for communicating incidents, failures, concerns, and other matters with internal and external parties.	Inspected the Incident Response Plan to determine that CoinDesk Indices has established standards for communicating incidents, failures, concerns, and other matters with internal and external parties.	No Exceptions Noted
CDI-2.2.2: Master License Agreements are established with external parties to provide the responsibilities, boundaries, confidentiality, and service levels to set expectations.	For a sample of new external parties, inspected their documented responsibilities and service levels in a Master License Agreement to determine that Master License Agreements are established with external parties to provide the responsibilities, boundaries, confidentiality, and service levels to set expectations.	No Exceptions Noted
CDI-3.1.1: CoinDesk Indices maintains a documented risk management program to consider the impact of internal and external factors to the organization.	Inspected the most recent risk assessment results and communication to ISC to determine that CoinDesk Indices maintains a documented risk management program to consider the impact of internal and external factors to the organization.	No Exceptions Noted

Management Control Activity	Test Procedures Performed by MHM	Results of Tests
CDI-3.1.2: CoinDesk Indices assesses third-party vendor risks prior to entering into an agreement and on an annual basis for critical or high risk vendors.	For a sample of new critical or high risk third-party vendors, inspected the completed risk review form and executed contract to determine CoinDesk Indices assesses third-party vendor risks prior to entering into an agreement for critical or high risk vendors. For a sample of existing critical or high risk third-party vendors, inspected the completed risk review form to determine CoinDesk Indices assesses third-party vendor risks on an annual basis for critical or high risk vendors.	No Exceptions Noted
CDI-4.1.1: CoinDesk Indices maintains a formal audit program that includes internal and external assessments which validate the implementation and operating effectiveness of corporate and IT controls.	Inspected the approved most recent audit plan to determine that CoinDesk Indices maintains a formal audit program that includes internal and external assessments which validate the implementation and operating effectiveness of corporate and IT controls.	No Exceptions Noted
CDI-5.1.1: From 1/1/2023 through 6/30/2023, system logs are collected and analyzed by the Security team on a biweekly basis for possible or actual attempts to breach the network.	For a sample of two weeks segments from 1/1/2023 through 6/30/2023, inspected the completed log review documentation to determine that system logs are collected and analyzed by the Security team on a biweekly basis for possible or actual attempts to breach the network.	For two out of two biweekly segments sampled, the system log review and analysis was not performed.
CDI-6.1.1: Password configuration settings are managed in compliance with the Password Standards Policy.	Inspected configured system password complexity requirements and Password Standards Policy to determine that password configuration settings are managed in compliance with the Password Standards Policy.	No Exceptions Noted
CDI-6.1.2: Multi-factor authentication is enforced for corporate applications and remotely accessing Amazon Web Services.	Inspected the multi-factor authentication settings for AWS management console and corporate applications to determine that multi-factor authentication is enforced for corporate applications and remotely accessing Amazon Web Services.	No Exceptions Noted
CDI-6.1.3: Administrative privileges to systems are limited to only appropriate and documented personnel.	Inspected user access listing for in-scope systems to determine that administrative privileges to systems are limited to only appropriate and documented personnel.	No Exceptions Noted

Management Control Activity	Test Procedures Performed by MHM	Results of Tests
CDI-6.2.1: Prior to issuing system credentials and granting system access, CoinDesk Indices documents and authorizes new users whose access is administered.	Inspected the CDI Provisioning Procedures to determine that prior to issuing system credentials and granting system access, CoinDesk Indices documents and authorizes new users whose access is administered. For a sample of new employees, inspected documented authorization to determine that prior to issuing system credentials and granting system access, CoinDesk Indices documents and authorizes new users whose access is administered.	No Exceptions Noted
CDI-6.2.2: Access is reviewed at a minimum on an annual basis. Any adjustments identified from the review presented to the Information Security Committee (ISC) are resolved.	Inspected the annual user access review to determine that users access privileges are reviewed annually by the Information Security Committee (ISC) and any adjustments identified from the review presented to the Information Security Committee (ISC) are resolved.	No Exceptions Noted
CDI-6.3.1: User system credentials are revoked in a timely manner upon notification of termination.	Inspected the CDI Provisioning Procedures to determine that user system credentials are revoked in a timely manner upon notification of termination. For a sample of terminated employees, inspected termination documentation and the user's system account status to determine that user system credentials are revoked in a timely manner upon notification of termination.	No Exceptions Noted For 2 of 3 terminated employees sampled, their user system credentials were not revoked timely.
CDI-6.5.1: Prior to reprovisioning or decommissioning, all digital media is completely sanitized to remove any data and software.	For a sample of reprovisioned and decommissioned assets, inspected sanitization documentation to determine that prior to reprovisioning or decommissioning, all digital media is completely sanitized to remove any data and software.	No Exceptions Noted

Management Control Activity	Test Procedures Performed by MHM	Results of Tests
CDI-6.5.2: Data is stored based on confidentiality requirements and access to that data follows defined user provisioning procedures.	Inspected CoinDesk Indices Data Classification Policy to determine that data is stored based on confidentiality requirements and access to that data follows defined user provisioning procedures. For a sample of new employees, inspected documented authorization to determine that prior to issuing system credentials and granting system access, CoinDesk Indices documents and authorizes new users whose access is administered.	No Exceptions Noted
CDI-6.7.1: A secured connection is utilized for external devices connecting to the AWS cloud environment.	Inspected VPN configurations to determine that a secured connection is utilized for external devices connecting to the AWS environment. Observed a user connect to the AWS cloud environment to determine that a secured connection is utilized for external devices.	No Exceptions Noted
CDI-6.7.2: Network policy rules are configured for externally facing assets to only allow specific services to specific destinations and all other services are not permitted.	Inspected the production firewall's network policy rules are configured for externally facing assets to only allow specific services to specific destinations and all other services are not permitted.	No Exceptions Noted
CDI-6.7.3: CoinDesk Indices employs a combination of TLS and HTTP (HTTPS) for the security of data transferred between CoinDesk Indices systems and client computers.	Inspected the security protocol configurations for websocket and API servers to determine that CoinDesk Indices employs a combination of TLS and HTTP (HTTPS) for the security of data transferred between CoinDesk Indices systems and client computers.	No Exceptions Noted
CDI-6.8.1: Anti-virus and malware protection is enforced on user workstations that connect to CoinDesk Indices assets. The software performs a complete scan on a daily basis.	Inspected the anti-virus and malware protection technical policies and configurations to determine that anti-virus and malware protection is enforced on user workstations and the software performs a complete scan on a daily basis. For a sample of employees that connect to CoinDesk indices assets, inspected the anti-virus and malware protection software management console to determine that the employees' laptop is managed by the tool.	No Exceptions Noted

Management Control Activity	Test Procedures Performed by MHM	Results of Tests
CDI-7.1.1: CoinDesk Indices maintains documented security standards for endpoints and systems that support the CoinDesk Indices products.	Inspected CDI's Security Standards document to determine that security standards are defined for endpoints and systems. For a sample of employees, inspected their laptop's endpoint security settings to determine that the endpoint is protected by the endpoint protection solution. For a sample of production systems, inspect the server's configurations to determine that server security standards were enabled.	No Exceptions Noted
CDI-7.1.2: Vulnerability assessments are conducted on a quarterly basis to identify security related issues or misconfigurations. Issues identified are reviewed by CoinDesk Indices personnel and tracked to resolution based on their assigned risk rating.	Inspect the vulnerability scanning tool's schedule and targeted systems to determine that vulnerability assessments are conducted on a quarterly basis to identify security related issues or misconfigurations. For a sample of quarters, inspected vulnerability resolution documentation to determine that vulnerability assessments are conducted on a quarterly basis and issues identified are reviewed by CoinDesk Indices personnel and tracked to resolution based on their assigned risk rating.	No Exceptions Noted
CDI-7.2.1: As of 7/1/2023, CDI enables a threat detection service that continuously monitors their production network for compromised accounts, anomalous behavior, and malware.	Inspected the threat detection service's configurations to determine that CDI enables a threat detection service that continuously monitors their production network for compromised accounts, anomalous behavior, and malware as of 7/1/2023.	No Exceptions Noted
CDI-7.3.1: Incidents are logged within a ticketing system, assigned a rating, and tracked to resolution.	For a sample of incidents, inspected documentation and tracking to determine that incidents are logged within a ticketing system, assigned a rating, and tracked to resolution.	No Exceptions Noted
CDI-8.1.1: CoinDesk Indices has a documented and approved change management policy that govern changes made to the production environment.	Inspected the approved change management policy to determine that CoinDesk Indices has a documented and approved change management policy that govern changes made to the production environment.	No Exceptions Noted

Management Control Activity	Test Procedures Performed by MHM	Results of Tests
CDI-8.1.2: Details related to a change are documented and retained.	For a sample of changes, inspected the change to determine that details related to a standard change are documented and retained.	No Exceptions Noted
CDI-8.1.3: Standard changes to the production environment are tested according to defined standards prior to migration.	For a sample of standard changes, inspected evidence of testing and the Change Management Policy to determine that standard changes to the production environment are tested according to defined standards prior to migration.	No Exceptions Noted
CDI-8.1.4: Standard changes are reviewed and approved prior to migration to the production environment. Emergency and configuration changes are reviewed andand approved after the change in production.	For a sample of changes, inspected evidence of review and approval to determine that standard changes are reviewed and approved in accordance with the change management procedures.	For 4 of 40 sampled changes, changes were not independently reviewed and approved before deploying to production.
CDI-8.1.5: CoinDesk Indices maintains separate production and development environments.	Inspected network configurations to determine that CoinDesk Indices maintains separate production and development environments.	No Exceptions Noted
AVAILABILITY		
CDI-A1.1.1: An enterprise monitoring system continuously monitors systems for capacity and usage of production systems. Defined tolerances are established and managed through CDI's change management process. Triggered alerts are monitored, managed and resolved by the operations team.	For a sample of production systems, inspected the established monitoring alert thresholds to determine that defined thresholds are established and an enterprise monitoring system continuously monitors systems for capacity and usage of production systems. Inspected the change management ticketing system to determine that changes to defined tolerances are managed through CDI's change management process. For a sample of triggered alerts, inspected the alert documentation to determine triggered alerts are monitored, managed and resolved by the operations team.	No Exceptions Noted
CDI-A1.1.2: Baseline rate limits have been defined on load balancers and within the application.	Inspected the load balancer configuration files to determine that baseline rate limits have been defined on load balancers and within the application.	No Exceptions Noted

Management Control Activity	Test Procedures Performed by MHM	Results of Tests
CDI-A1.2.1: Backups of critical AWS CoinDesk Indices systems are maintained and monitored for successful replication across multiple devices.	Inspected the automated backup schedule to determine that backups of critical CoinDesk Indices systems are maintained and replicated across multiple devices. For a sample of failed backups, inspected monitoring alerts, backup statuses and/or investigation tickets to determine that backup failures are monitored.	No Exceptions Noted The operating effectiveness of the control related to monitoring could not be tested because there were no backup failures during the audit period.
CDI-A1.2.2: Critical system components are replicated across multiple availability zones.	For a sample of critical system components, inspected its AWS replication configurations to determine that critical system components are replicated across multiple availability zones.	No Exceptions Noted
CDI-A1.3.1: Data backup restoration is validated and tested on an annual basis.	Inspected completed documentation for the annual data backup restoration tests to determine that data backup restoration is validated and tested on an annual basis.	No Exceptions Noted
CDI-A1.3.2: Business Continuity and Disaster Recovery plans are documented and tested on an annual basis in accordance with CoinDesk Indices' system availability standards.	Inspected the Business Continuity and Disaster Recovery plans to determine that they are documented. Inspected the completed annual Business Continuity and Disaster Recovery test and results to determine that Business Continuity and Disaster Recovery plans are tested on an annual basis in accordance with CoinDesk Indices' system availability standards.	No Exceptions Noted

Section 5

Other Information Provided by
CoinDesk Indices, Inc.

Section 5 - Other Information Provided by CoinDesk Indices, Inc.

The information in section 5 is presented by management of CoinDesk Indices, Inc. to provide additional information and is not a part of CoinDesk Indices, Inc.'s description of its Digital Currency Index Platform system during the period January 1, 2023 to December 31, 2023. Information about CoinDesk Indices, Inc.'s response to exceptions has not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it. However, we noted that information in section 5 is materially consistent with CoinDesk Indices, Inc.'s description of its Digital Currency Index Platform System.

Management's Response to Testing Exceptions

Management's Control Activity #	Management's Control Activity Description	Testing Procedures Performed by MHM	Results of Tests
CDI-5.1.1	From 1/1/2023 through 6/30/2023, system logs are collected and analyzed by the Security team on a biweekly basis for possible or actual attempts to breach the network.	For a sample of two weeks segments from 1/1/2023 through 6/30/2023, inspected the completed log review documentation to determine that system logs are collected and analyzed by the Security team on a biweekly basis for possible or actual attempts to breach the network.	For 2 out of 2 biweekly segments sampled, the system log review and analysis was not performed.
Management response: We acknowledge and accept the finding of the audit team that there was a lapse in performing bi-weekly system log reviews and analysis. During this period, there was a departure in key security staffing resulting in a lapse of bi-weekly reviews during the transition. Post departure CoinDesk Indices implemented a project to streamline and provide enhanced real-time monitoring and alerting. In addition, multiple staff are now notified in the event of a possible or actual attempts to breach the network. CoinDesk Indices will take efforts to continue to improve our security monitoring and alerting such as establishing a dedicated Security Operation Center.			

Management's Control Activity #	Management's Control Activity Description	Testing Procedures Performed by MHM	Results of Tests
CDI-6.3.1	User system credentials are revoked in a timely manner upon notification of termination.	Inspected the CDI Provisioning Procedures to determine that user system credentials are revoked in a timely manner upon notification of termination. For a sample of terminated employees, inspected termination documentation and the user's system account status to determine that user system credentials are revoked in a timely manner upon notification of termination.	No Exceptions Noted For 2 of 3 terminated employees sampled, their user system credentials were not timely revoked.
Management response: We acknowledge and accept the finding of the audit team that 2 of 3 system credentials for terminated employees were not revoked in a timely manner. CoinDesk Indices noted the finding during the period and took steps to perform an internal audit all terminated employee accounts within the period to ensure access was revoked. In addition, a new IT manager was brought onboard and has since developed a new standard procedure to ensure employee access is completely removed in a timely manner.			

Management's Control Activity #	Management's Control Activity Description	Testing Procedures Performed by MHM	Results of Tests
CDI-8.1.4	Standard changes are reviewed and approved prior to migration to the production environment. Emergency and configuration changes are reviewed and approved after the change in production.	For a sample of changes, inspected evidence of review and approval to determine that standard changes are reviewed and approved in accordance with the change management procedures.	For 4 of 40 sampled changes, changes were not independently reviewed and approved before deploying to production.
Management response: We acknowledge and accept the finding of the audit team that 4 of 40 sampled changes were not independently reviewed and approved before deploying to production. We initiated a retrospective review of the 4 changes identified to assess and mitigate any potential risks. We are committed to further strengthening our change management procedures, which were comprehensively updated in the third quarter of 2023. We will further reinforce these standards to ensure staff adhere to established escalation, review, and approval procedures. In addition, CoinDesk Indices has started a project to implement controls to further reduce the number of employees that can commit changes to the production environment.			