CIVILIZED DISCOURSE CONSTRUCTION KIT, INC.

SOC 2 REPORT

FOR THE

DISCOURSE SOFTWARE AS A SERVICE (SAAS) SYSTEM

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S
REPORT ON CONTROLS RELEVANT TO SECURITY

OCTOBER 1, 2021, TO MAY 31, 2022

PREPARED IN ACCORDANCE WITH THE
AICPA SSAE NO. 18 AND IAASB ISAE 3000 STANDARDS

Attestation and Compliance Services

This report is intended solely for use by the management of Civilized Discourse Construction Kit, Inc., user entities of Civilized Discourse Construction Kit, Inc.'s services, and other parties who have sufficient knowledge and understanding of Civilized Discourse Construction Kit, Inc.'s services covered by this report (each referred to herein as a "specified user").

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Table of Contents

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Civilized Discourse Construction Kit, Inc.:

Scope

We have examined Civilized Discourse Construction Kit, Inc.'s ("CDCK" or the "service organization") accompanying description of its Discourse Software as a Service (SaaS) system, in Section 3, throughout the period October 1, 2021, to May 31, 2022, (the "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"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2021, to May 31, 2022, to provide reasonable assurance that CDCK's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

CDCK uses various subservice organizations for data center and cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CDCK, to achieve CDCK's service commitments and system requirements based on the applicable trust services criteria. The description presents CDCK's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of CDCK's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

CDCK 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 CDCK's service commitments and system requirements were achieved. CDCK has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. CDCK 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.

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 (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated 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 and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the 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; and
- Evaluating the overall presentation of the description.

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

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report 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 the policies or procedures may deteriorate.

Description of Test of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in Section 4 of our report titled "Testing Matrices."

Opinion

In our opinion, in all material respects:

a. the description presents CDCK's Discourse SaaS system that was designed and implemented throughout the period October 1, 2021, to May 31, 2022, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period October 1, 2021, to May 31, 2022, to provide reasonable assurance that CDCK'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 organizations applied the complementary controls assumed in the design of CDCK's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period October 1, 2021, to May 31, 2022, to provide reasonable assurance that CDCK's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of CDCK'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 CDCK; user entities of CDCK's Discourse SaaS system during some or all of the period of October 1, 2021, to May 31, 2022, business partners of CDCK subject to risks arising from interactions with the Discourse SaaS 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 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; and
- 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 these specified parties.

Schellman & Company, LLC

Columbus, Ohio
June 27, 2022

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of CDCK's Discourse SaaS system, in Section 3, throughout the period October 1, 2021, to May 31, 2022, (the "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 Discourse SaaS system that may be useful when assessing the risks arising from interactions with CDCK's system, particularly information about system controls that CDCK has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

CDCK uses various subservice organizations for data center and cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CDCK, to achieve CDCK's service commitments and system requirements based on the applicable trust services criteria. The description presents CDCK's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of CDCK's controls. The description does not disclose the actual controls at the subservice organizations.

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

a. the description presents CDCK's Discourse SaaS system that was designed and implemented throughout the period October 1, 2021, to May 31, 2022, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period October 1, 2021, to May 31, 2022, to provide reasonable assurance that CDCK'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 organizations applied the complementary controls assumed in the design of CDCK's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period October 1, 2021, to May 31, 2022, to provide reasonable assurance that CDCK's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of CDCK's controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

Overview of Operations

Company Background

Civilized Discourse Construction Kit, Inc. (CDCK) was founded in 2013 by three co-founders with an interest in online discussion. Their primary objective was to provide a community platform for civilized discussion on the web. CDCK is a hosting company that develops and hosts Discourse, a 100% open-source software project.

CDCK is a completely remote company, working from 19 countries, 15 time zones and uses Discourse as the primary team coordination tool to build Discourse. Discourse excels at asynchronous, distributed teamwork, so interruptions such as instant messaging, calls, and meetings are kept to a minimum.

Description of Services Provided

CDCK provides a 100% open-source discussion platform built for the next decade of the Internet. The platform can be used as a mailing list, discussion forum, long-form chat room, and more. Discourse is a from-scratch reboot; an attempt to reimagine what a modern Internet discussion platform should be today in a world of ubiquitous smartphones, tablets, and social media. CDCK provides a hosting service for Discourse, either on its redundant co-located servers in Fremont, California, USA; Dublin, Ireland; Seattle, Washington, USA; Toronto, Ontario, Canada; or cloud hosted on Amazon Web Services (AWS).

Principal Service Commitments and System Requirements

CDCK designs its processes and procedures to meet its objectives for its Discourse SaaS system. Those objectives are based on the service commitments that CDCK makes to user entities and the laws, regulations, and compliance requirements that CDCK has established for the services.

CDCK's commitments to their customers related to security are documented and communicated in customer agreements. CDCK's commitments include the following:

- Maintain administrative and technical safeguards to protect the security of databases and customer data.
- Protect data at rest and in transit.
- Take industry-standard security precautions to defend the Discourse SaaS from malicious technical attack and data compromise.
- Prevent the access, use, or disclosure of customer data without permission.
- Respond to customer support requests from customer personnel via e-mail about configuration of, use of, and problems with the Discourse SaaS.
- Ensure employees keep customer data confidential and take security precautions.
- Ensure the latest version of Discourse and Discourse plugins are free of computer viruses, trojans, worms, and other malicious code.

CDCK has also established system requirements that support the achievement of the principal service commitments. These requirements include the following:

- Information security policies to guide CDCK personnel in the protection of information assets and data;
- Procedures for provisioning access to in-scope systems on a need-to-know basis, performing periodic access reviews, and managing credentials;
- Employee provisioning and deprovisioning standards;

- Minimum password standards;
- Periodic access reviews;
- Data handling and encryption policies and procedures;
- Encryption standards for data at transit and at rest;
- System logging, monitoring, and alerting;
- Incident handling standards;
- Change management standards;
- Vendor management;
- Security awareness training;
- Employee acknowledgement of security policies;
- Sanction procedures for misconduct; and
- Endpoint security monitoring.

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

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure and Software

CDCK's production infrastructure supporting the Discourse SaaS system is hosted within multiple physical data center facilities for metal infrastructure and within the cloud via AWS. A Hurricane Electric (HE) facility in Fremont, California, USA, and Equinix facilities in Dublin, Ireland; Seattle, Washington, USA; and Toronto, Ontario, Canada, provide data center services, while the cloud infrastructure is located in multiple AWS availability zones in us-west-1 (Northern California), plus multiple other regions to support specific deployments as requested by customers. Production servers and client-facing applications are logically and physically segmented from CDCK's internal information systems. Puppet is utilized for system configuration orchestration and globally manages access to both metal and cloud production resources.

[Intentionally Blank]

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
Firewall System	Firewall system configured to protect the network perimeter and limit inbound and outbound access.	Shorewall / iptables (HE and Equinix)	HE Equinix AWS
		Security Groups (AWS)	
Servers	Infrastructure to support the Discourse SaaS.	Linux	
Containers	Operating system virtualization utilized to create, package, and run applications.	Docker	
PostgreSQL	Underlying relational database management system (DBMS) used to support the Discourse SaaS.	PostgreSQL	
Discourse	Core product application software.	Linux	

Secondary Infrastructure and Supporting Software

The following secondary infrastructure and supporting software is utilized in support of the delivery of the service:

- GitHub – source code management software utilized to control code versioning, automated code testing, and security through the code development process.
- Puppet – system configuration orchestration and globally management of access to both metal and cloud production resources.
- Ecrasite – internally developed tool utilized to regularly scan deployed container images to identify software vulnerabilities.
- Detectify – automated web vulnerability scanning tool utilized to identify software vulnerabilities for the Discourse website and Discourse meta forum.
- HackerOne – vulnerability coordination and bug bounty platform utilized to surface security issues and vulnerabilities by leveraging external users.
- Zoho Vault – secure password manager that stores, manages, and controls access to passwords across websites and applications.
- Linux Unified Key Setup (LUKS) – utilized for full disk encryption for block devices and disk volumes and converts data into unreadable code that requires a unique encryption passphrase.
- Kolide – endpoint security monitoring for remote devices.

People

CDCK has a staff of employees organized in the following functional areas:

- Executive management – Senior management providing general oversight and strategic direction for operations.
- Software engineering team – Responsible for developing the Discourse application, customizing it to fit customers' needs, and migrating customer data from other platforms onto Discourse.
- Infrastructure team – Responsible for building, managing, and maintaining CDCK hardware and infrastructure.
- Technical advocacy team – Responsible for technical and customer support.
- Finance team – Responsible for accounts payable, receivable and accounting compliance.

- Legal team – Responsible for legal and privacy compliance.
- Design team – Responsible for the design of the core product and consultancy to customers.
- Customer success team – Responsible for interfacing with large enterprise customers.
- HR team – Responsible for human resource functions.
- Business team – Responsible for business management functions.

Procedures

Access, Authentication, and Authorization

Access to system information, including confidential data, is protected by authentication and authorization mechanisms. Standard procedures require the access control systems to enforce logical access to production servers and applications. Additionally, the production environment is segmented from other non-critical environments to ensure that confidential data is isolated from unrelated networks.

Users accessing production systems are required to be granted access to Puppet and authenticate utilizing a unique user account and Secure Shell (SSH) public key with minimum password requirements. Puppet users' unique encrypted passwords are stored within Puppet, and passwords for additional administrative accounts are stored within a secure password manager accessible only by authorized personnel. Production servers can be accessed by authenticated Puppet users via SSH public key authentication. For database access, users must be authenticated to servers prior to accessing any PostgreSQL databases. Additionally, a security token service (STS) client is utilized to validate AWS credentials and generate a security token for multi-factor authentication (MFA) that allows access to resources based on the user's role. Users can also access the AWS management console via identity access management (IAM) credentials including a unique username, password, and MFA. MFA is also required to authenticate to the Discourse application. Users are added to predefined user access groups to ensure role-based access privileges are enforced and access to data is segregated.

Administrative access privileges to in-scope systems are assigned to only those users requiring access to fulfill their job responsibilities. User-specific keys and master / root account passwords are stored in an encrypted format within Puppet and the internal Discourse system. Passwords are stored in an encrypted format and accessible by authorized engineering and development personnel.

Access Requests and Access Revocation

A formal process is established for managing user accounts and controlling access to CDCK's resources. User access requests are documented using Discourse and require the approval of a manager. User access reviews, including a review of privileged users, are performed quarterly by infrastructure team personnel to help ensure that access to data is restricted to authorized personnel.

Upon notification of an employee termination, a revocation request is communicated within the Discourse application for the removal of access to in-scope systems. Upon receipt of the notification, infrastructure personnel remove or disable applicable system access for the terminated employee.

Workstation Security

Kolide endpoint security software is utilized to manage and secure employee workstations by centrally auditing full disk encryption, antivirus, threat protection settings, and automatic software updates to Windows and MacOS workstations.

Physical Security

Physical servers and infrastructure supporting the Discourse system are housed in the HE data center facility in Fremont, California, and in Equinix data center facilities located in Dublin, Ireland; Seattle, Washington; and Toronto, Canada. CDCK maintains a listing of individuals authorized to access the data center facilities and quarterly physical access reviews are performed by infrastructure team personnel to help ensure that access to data center facilities is restricted to authorized CDCK personnel.

Physical access controls related to the third-party data center facilities are the responsibility of the third-party provider.

Change Management

CDCK's change management policies and procedures guide personnel in the initiation, ownership, responsibility, and documentation of changes. The Discourse SaaS system and version control software are utilized to document, manage, and monitor changes from change request through implementation. Discussions take place within the Discourse forum as needed throughout the change lifecycle, and it is the responsibility of the change owner to document important information in a topic as well as understand the potential impact of production changes on systems and customers.

Application code changes are required to pass automated testing checks within the version control software prior to being merged to the main branch. Infrastructure changes do not require testing; however, testing may be performed depending on the nature of the change. Upon completion of successful testing, changes are approved prior to implementation to the production environment.

Version control software is utilized to maintain source code versions, manage the lifecycle of source code from the development process to the implementation / installation within the production environment, and restrict access to modify application source code to authorized personnel. The version control software maintains a history of code changes to support rollback capabilities and tracks changes and change activities by user account. In addition, branch protections enforce code review and approval by an individual independent from the author of the change prior to merging code to the main branch. Administrative access privileges within the version control software are restricted to user accounts accessible by authorized engineering and management personnel.

Changes are implemented to the production environment by authorized personnel who do not have code development responsibilities after the requisite steps of the change management lifecycle are completed.

Incident Response

A documented incident response plan, that is tested at least annually, is in place to guide personnel in the escalation, communication, response, and remediation of security incidents. Documented escalation procedures for reporting security incidents are provided to employees to guide them in identifying and reporting failures, incidents, concerns, and other complaints. Incidents may be triggered by automated monitoring systems or manually by personnel or external users. CDCK categorizes incidents based on their severity. A "PRI-1" incident is classified as a major incident that could result in the system being in a critical state, system functionality impaired for a time period breaking the service level agreement, or customer data exposure. A "PRI-2" incident is slightly less severe and could cause performance issues that negatively impact a small group of customers. "PRI-3" and "PRI-4" category incidents are considered to be minor and do not require the initiation of the incident response process. The Discourse application is utilized as a ticketing system to document security incidents, response, and resolution activities. Postmortem evaluations are completed for critical security incidents to help ensure corrective measures are implemented. Incidents requiring a change to the system follow the standard change control process.

System Monitoring

CDCK utilizes the HackerOne bug bounty program service for vulnerability assessments of in-scope systems to identify threats and assess their potential impact to system security. Critical security findings identified as a result of the assessments are triaged by the security team and monitored through resolution. Additionally, security monitoring applications are utilized to monitor and analyze live container images and the Discourse website for any production image and web vulnerabilities, including any possible or actual security breaches. Identified security vulnerabilities are triaged by security personnel and monitored through resolution.

In addition to vulnerability scanning and security event monitoring, CDCK utilizes a third-party specialist to perform annual penetration testing of in-scope systems. Management reviews the results of the penetration tests and remediation plans are proposed and monitored through resolution, as applicable.

Data

Each CDCK location has data stored in PostgreSQL databases that are encrypted at rest and in transit. Infrastructure that houses data is either in metal infrastructure at the HE data center facilities in Fremont, California, or Equinix data center facilities in Dublin, Ireland; Seattle, Washington; and Toronto, Canada; or within AWS throughout multiple availability zones to ensure the failure of any single server or zone would not result in the loss of data.

Traffic enters the Discourse SaaS environment through dedicated private servers that route the data across the infrastructure. Log-related data is moved off of individual webservers and stored centrally in an elastic search service.

Equinix and HE do not process data for CDCK and do not have access to CDCK customer data. HE provides Internet transit for CDCK, and data flows through the HE networking gear, but data is not processed beyond what is necessary for IP packet forwarding.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data	**Data Description**	**Classification**
Customer information	Information provided to CDCK by the customer.	Confidential
Business information	Information that CDCK has created, generated, or collected, which is not intentionally made available to the public.	

Significant Changes During the Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

Subservice Organizations

The data center services provided by HE and Equinix and cloud hosting services provided by AWS were not included within the scope of this examination.

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

Control Activities Expected to be Implemented by HE, Equinix, and AWS	Applicable Trust Services Criteria
AWS is responsible for implementing controls that ensure logical access to the underlying network and virtualization management software is managed for its cloud hosting services where in-scope systems reside.	CC6.1 – CC6.3 CC6.5 – CC6.6
HE, Equinix, and AWS are responsible for implementing controls that ensure physical access to facilities and system components including firewalls, routers, and servers is restricted to authorized personnel.	CC6.4 – CC6.5

CONTROL ENVIRONMENT

The control environment at CDCK is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors and information security management committee (ISMC).

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of CDCK's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of CDCK's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. Management formally documents and reviews the employee handbook containing the code of conduct annually that communicates CDCK's values and behavioral standards to personnel. Upon hire, and annually thereafter, employees are required to acknowledge the code of conduct and understand their responsibility for adhering to CDCK's behavioral standards. Specific control activities that the service organization has implemented in this area are described below:

- Management formally documents, and reviews annually, the organizational policy statements that communicate CDCK's values and behavioral standards to personnel.
- Employees are required to acknowledge upon hire, and at least annually thereafter, that they have been given access to the employee handbook and code of conduct and understand their responsibility for adhering to CDCK's behavioral standards.
- Employees are required to sign a confidentiality statement annually agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- Background checks and employee skills assessment are performed for employees as a component of the hiring process.

Board of Directors and ISMC Oversight

The board of directors works together with the ISMC to assist with the communication of audit results and the enforcement of internal policies. The ISMC consists of one member of executive management, one member of human resources, two members of the infrastructure team, and one executive assistant who are responsible for setting company objectives and overseeing performance of internal controls. The ISMC's responsibilities include reviewing internal policies, audit planning, coordination, and assessment of results. The ISMC meets quarterly to discuss and align internal control responsibilities, performance measures, and incentives with company objectives. The ISMC reports to the board of directors and communicates with executive and operational management regarding the results of audit reports.

The board of directors consists of members independent of CDCK management to exercise oversight for organizational objectives as well as the system of internal control.

Organizational Structure and Assignment of Authority and Responsibility

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

CDCK's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established.

It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand CDCK's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Specific control activities that the service organization has implemented in this area are described below:

- Documented job descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs and communicated to employees through the CDCK intranet.
- Management reviews job descriptions annually and makes updates, if necessary.
- An ISMC is in place to formulate and guide CDCK's strategy and manage security risks.

Commitment to Competence

CDCK's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge as well as attracting, developing, and retaining competent individuals. Specific control activities that the service organization has implemented in this area are described below:

- New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.
- Documented job descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs, and are communicated to employees through the CDCK intranet.
- Employment candidates' qualifications are assessed as a component of the hiring process to determine if the candidate possesses the required qualifications to perform the duties as outlined in the job description.
- Management conducts an annual performance review of employees to evaluate the individual's performance against expected levels.
- Employees are required to complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate security policies.
- Management personnel monitor compliance with training requirements annually.

Accountability

Management establishes accountability by setting a strong tone at the top and holding those accountable for internal control responsibilities. Management establishes and communicates both policy ownership and internal control responsibilities and evaluates ownership, responsibility, and performance of internal controls on a frequent basis. Specific control activities that the service organization has implemented in this area are described below:

- Management formally documents, and reviews annually, the organizational policy statements that communicate CDCK's values and behavioral standards to personnel.
- Internal control responsibilities regarding security are documented within the information security policies. Employees are required to acknowledge that they have read and understand their responsibilities upon hire and annually thereafter.
- Documented job descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs and communicated to employees through the CDCK intranet.
- Management conducts an annual performance review of employees to evaluate the individual's performance against expected levels.
- An employee sanction procedure is documented within the employee handbook communicating that an employee could face disciplinary action, up to and including termination of employment, for noncompliance with a policy and/or procedure.

RISK ASSESSMENT

Objective Setting

The risk assessment process involves a dynamic process that includes identification and analysis of risks that pose a threat to CDCK's ability to perform the in-scope services or achieve its security principal service commitments. The process first starts with determining the organization's objectives and commitments as these are key to understanding the risks and allows for the identification and analysis of those risks relative to the objectives and commitments. It is the responsibility of any CDCK employee to identify risks per the risk assessment policy, and it is a risk owner's responsibility to evaluate, monitor, and communicate risks associated with any activity, technology, function, or process within their relevant scope of responsibility and authority.

Risk Identification and Analysis

CDCK's risk assessment policy and procedures describe the methodology that CDCK has in place to identify assets; assess internal and external threats and vulnerabilities of the assets; process risks including technical risks; and identify how those risks are evaluated, assessed, treated, and mitigated. The risk assessment is performed and reviewed at least annually to identify threats and vulnerabilities that could impede the achievement of the security principal service commitments, but the identification of risks, treatment, and performance of mitigating controls are ongoing processes.

Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud, fraud incentives, pressures, and opportunities for employees, and employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired and methods of training utilized
- Changes in management responsibilities

Potential for Fraud

Management considers the potential for fraud when assessing the risks to CDCK's objectives. Management realizes that the potential for fraud can occur in several forms including when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Documented policies and procedures are in place to

guide personnel in identifying the potential for fraud when performing the risk assessment process. The annual risk assessment process considers the potential for fraud. Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review.

Vendor Risk Management

CDCK relies on vendors to perform a range of services and aims to manage its relationship with vendors and minimize the risks associated with engaging vendors to perform services. CDCK has implemented a vendor management policy that provides a framework for managing the lifecycle of vendor relationships and addressing security risks related to vendors. Risks arising from the use of vendors providing goods and services are analyzed as part of the annual risk assessment. Vendors and third parties are required to enter an agreement with CDCK for services provided that includes statements of confidentiality. Additionally, compliance personnel evaluate vendor risk and relevant compliance reports for high-risk vendors annually to help ensure that third-party vendors comply with CDCK's security requirements.

Risk Mitigation

Upon the identification, evaluation, and analysis of risks, risk treatment options are considered and established. This involves judgment based on assumptions about the risk and reasonable analysis associated with reducing the level of risk. Management establishes tolerable risk levels based on the probability of threat materialization and the cost of implementing measures to reduce risk. Per the risk assessment policy, the possible range of treatments can be broken down into the following categories: elimination, mitigation, acceptance, transference, and avoidance. Necessary actions are taken to reduce the impact or likelihood of the risk occurring, including the identification of the mitigating control activities.

Trust Services Criteria and Related Control Activities

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security category.

Selection and Development of Control Activities

Selecting control activities includes consideration of the relevant business processes, security commitments, and identified risks that require control activities. Documented policies and procedures are in place to guide personnel in performing the risk assessment process that include the development of risk treatment plans to mitigate identified risks. As an output to the risk assessment process, mitigating controls and risk response plans are documented. Additional control activities may be designed as a result of the risk assessment to further mitigate identified risks. Executive management establishes key performance indicators (KPIs) to evaluate internal control effectiveness, including the acceptable level of control operation and failure. Risk owners are responsible for selecting and monitoring mitigating controls for the risks in which they are assigned.

Control activities are deployed through the use of policies to establish what is expected and procedures that put policies into action. Security policies are formally documented and enforced to guide employees, and an employee sanction procedure is documented within the employee handbook communicating that an employee could face disciplinary action, including termination of employment, for noncompliance with a policy and/or procedure.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security category are applicable to the Discourse SaaS system.

INFORMATION AND COMMUNICATION SYSTEMS

Pertinent information must be identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Policies and procedures are in place to guide employees in providing effective communication to both internal and external parties. Information systems also produce reports that make it possible to run and control the business. CDCK deals not only with internally generated data, but also information about external events, activities, and conditions necessary to inform business decision-making and external reporting. Effective communication must occur throughout the organization and to external parties to achieve objectives and principal service commitments. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others.

Internal Communications

CDCK has implemented various methods of internally communicating information including objectives and responsibilities for internal control necessary to support the functioning of internal control. Specific control activities that CDCK has implemented in this area are described below.

- Documented policies and procedures are in place to guide personnel in areas including, but not limited to, the following:
    - Information Security;
    - Data Retention and Destruction;
    - Logical Access; and
    - Change Management.
- Internal control responsibilities regarding security are documented within the information security policies. Employees are required to acknowledge that they have read and understand their responsibilities upon hire and annually thereafter.
- Employees are required to complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate security policies.
- Documented job descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs, and are communicated to employees through the CDCK intranet.
- Documented escalation procedures for reporting security incidents are provided to internal users to guide them in identifying and reporting failures, incidents, concerns, and other complaints.
- Employees are required to acknowledge, upon hire and at least annually thereafter, that they have been given access to the employee handbook and code of conduct and understand their responsibility for adhering to CDCK's behavioral standards.
- Executive management meetings are held with operational management at least annually to discuss and align internal control responsibilities, performance measures, and incentives with company objectives.
- Reporting procedures are in place to facilitate the reporting of complaints, unethical behaviors, and fraudulent activities.

External Communications

CDCK has also implemented various methods of communicating with external parties regarding matters affecting the functioning of internal control. Specific control activities that CDCK has implemented in this area are described below.

- CDCK's security commitments and the associated system requirements are documented in the enterprise hosting terms.
- System components, planned outages, and known issues are communicated to external parties via the company website.
- Vendors and third parties are required to enter an agreement with CDCK for services provided that includes statements of confidentiality.
- Communication channels are in place to enable external parties to report security incidents, concerns, and complaints.
- CDCK contact information and relevant communication channels are available to external parties via the public-facing website.

MONITORING

Monitoring is a process that assesses the quality of internal controls' performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing monitoring, separate evaluations, and monitoring of CDCK's subservice organizations. Monitoring activities also include using information from communications with external parties such as user customer complaints and regulatory comments that may indicate problems or highlight areas in need of improvement.

Ongoing Monitoring

CDCK has selected, developed, and implemented ongoing monitoring procedures to ascertain whether the components of internal controls are present and functioning. HackerOne vulnerability assessments of in-scope systems are performed on a continuous basis to identify threats and assess their potential impact to system security. Identified security findings classified as 'critical' are triaged by the security team and monitored through to resolution. Security applications are in place to monitor and analyze the in-scope systems for security vulnerabilities to production images and the Discourse website, including any possible or actual security breaches. Identified security vulnerabilities are triaged by the security team and monitored through to resolution.

Separate Evaluations

Security and compliance personnel obtain penetration testing reports annually as evidence that a third-party specialist performed penetration testing. Management reviews the results of the penetration tests and remediation plans are proposed and monitored through resolution. The audit committee, composed of executive management personnel, performs internal audits annually to identify potential control gaps and weaknesses. Management reviews results of third-party audits at least annually. CDCK process owners and management are continuously developing processes, controls, and policies to address risks that threaten service commitments.

Subservice Organization Monitoring

CDCK has implemented monitoring activities over services provided by vendors supporting the Discourse SaaS system. The compliance team evaluates vendor risk and reviews vendor compliance reports annually to help ensure that third-party vendors comply with CDCK's security requirements. The reviews include an assessment of vendor risk from numerous perspectives including compliance risk, strategic risk, operational risk, and reputational risk. For vendors considered to be high risk, an additional review of compliance reports is performed.

Evaluating and Communicating Deficiencies

Deficiencies in CDCK's internal control system can surface from many sources including the company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to ensure internal control deficiencies are reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to management personnel. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Corrective action is taken, as necessary, and modifications to controls may be implemented to ensure that current processes are reflected to mitigate risks.

COMPLEMENTARY CONTROLS AT USER ENTITIES

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Discourse SaaS system provided by CDCK. The scope of the testing was restricted to the Discourse SaaS system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period October 1, 2021, to May 31, 2022.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by subservice organizations in order to complement the control activities and achieve the applicable trust services criteria are presented in the "Subservice Organizations" section within Section 3.

SECURITY CATEGORY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Environment			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Management formally documents, and reviews annually, the organizational policy statements that communicate Discourse's values and behavioral standards to personnel.	Inspected code of conduct and evidence of management review during the period to determine that management formally documented and reviewed the organizational policy statements that communicated Discourse's values and behavioral standards to personnel.	No exceptions noted.
CC1.1.2	Employees are required to acknowledge, upon hire and at least annually thereafter, that they have been given access to the employee handbook and code of conduct and understand their responsibility for adhering to Discourse's behavioral standards.	Inspected the employee handbook acknowledgement for a sample of employees hired during the period to determine that each employee sampled acknowledged the employee handbook upon hire.	No exceptions noted.
		Inspected the employee handbook acknowledgement for a sample of current employees to determine that each employee sampled acknowledged the employee handbook during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.3	Employees are required to sign a confidentiality statement annually agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the signed confidentiality agreement for a sample of current employees to determine that each employee sampled signed a confidentiality statement during the period agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
CC1.1.4	Background checks and employee skills assessments are performed for employees as a component of the hiring process.	Inspected the background check and employee skills assessment for a sample of employees hired during the period to determine that a background check and employee skills assessment was performed for each employee sampled as a component of the hiring process.	No exceptions noted.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	The board of directors has members who are independent from CDCK management and objective in evaluations and decision making.	Inspected the board of directors' membership listing to determine that the board of directors had members who were independent from CDCK management.	No exceptions noted.
CC1.2.2	ISMC meetings are held with executive management quarterly to discuss and align internal control responsibilities, performance measures, and incentives with company objectives.	Inspected the ISMC meeting agenda for a sample of quarters during the period to determine that ISMC meetings were held with executive management to discuss and align internal control responsibilities, performance measures, and incentives with company objectives for each quarter sampled.	No exceptions noted.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	Documented job descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs, and are communicated to employees through the Discourse intranet.	Inspected the job descriptions for a sample of current employees and evidence of communication of job descriptions via the Discourse intranet to determine that documented job descriptions were in place for each employee sampled to define the skills, responsibilities, and knowledge levels required for particular jobs, and were communicated to employees through the Discourse intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3.2	Management reviews position descriptions annually and makes updates, if necessary.	Inspected evidence of management's review of job description during the period to determine that management reviewed job descriptions during the period and made updates, if necessary.	No exceptions noted.
CC1.3.3	An ISMC has been established to formulate and guide Discourse's strategy and manage security risks.	Inspected the ISMC Discourse topic to determine that an audit committee was established to formulate and guide Discourse's strategy and manage security risks.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	Inspected the hiring and onboarding procedure to determine that new employee hiring procedures were in place to guide the hiring process and included verification that candidates possessed the required qualifications to perform the duties as outlined in the job description.	No exceptions noted.
CC1.4.2	Documented job descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs, and are communicated to employees through the Discourse intranet.	Inspected the job descriptions for a sample of current employees and evidence of communication of job descriptions via the Discourse intranet to determine that documented job descriptions were in place for each employee sampled to define the skills, responsibilities, and knowledge levels required for particular jobs, and were communicated to employees through the Discourse intranet.	No exceptions noted.
CC1.4.3	Employment candidates' qualifications are assessed as a component of the hiring process to determine if the candidate possesses the required qualifications to perform the duties as outlined in the job description.	Inspected the employee skills assessment for a sample of employees hired during the period to determine that employment qualifications were assessed for each employee sampled.	No exceptions noted.
CC1.4.4	Management conducts an annual performance review of employees to evaluate the employees against expected levels of performance and conduct.	Inspected the most recent performance review completed for a sample of current employees to determine that management conducted a performance review during the period for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.5	Employees are required to complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate security policies.	Inspected security awareness training completion records for a sample of employees hired during the period to determine that each employee sampled completed security awareness training upon hire.	No exceptions noted.
		Inspected security awareness training completion records for a sample of current employees to determine that each employee sampled completed security awareness training during the period.	No exceptions noted.
CC1.4.6	Management personnel monitor compliance with training requirements annually.	Inspected evidence of training completion monitoring to determine that management personnel monitored compliance with training requirements during the period.	No exceptions noted.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Management formally documents, and reviews annually, the organizational policy statements that communicate Discourse's values and behavioral standards to personnel.	Inspected code of conduct and evidence of management review during the period to determine that management formally documented and reviewed the organizational policy statements that communicated Discourse's values and behavioral standards to personnel.	No exceptions noted.
CC1.5.2	Internal control responsibilities regarding security are documented within the information security policies. Employees are required to acknowledge that they have read and understand their responsibilities upon hire and annually thereafter.	Inspected the information security policies and the policy acknowledgement for a sample of employees hired during the period to determine that internal control responsibilities regarding security were documented within the information security policies and that each employee sampled acknowledged the policies upon hire.	No exceptions noted.
		Inspected the information security policies and the policy acknowledgement for a sample of current employees to determine that internal control responsibilities regarding security were documented within the information security policies and that each employee sampled acknowledged the policies during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.3	Documented job descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs, and are communicated to employees through the Discourse intranet.	Inspected the job descriptions for a sample of current employees and evidence of communication of job descriptions via the Discourse intranet to determine that documented job descriptions were in place for each employee sampled to define the skills, responsibilities, and knowledge levels required for particular jobs, and were communicated to employees through the Discourse intranet.	No exceptions noted.
CC1.5.4	Management conducts an annual performance review of employees to evaluate the employees against expected levels of performance and conduct.	Inspected the most recent performance review completed for a sample of current employees to determine that management conducted a performance review during the period for each employee sampled.	No exceptions noted.
CC1.5.5	An employee sanction procedure is documented within the employee handbook communicating that an employee could face disciplinary action, including termination of employment, for noncompliance with a policy and/or procedure.	Inspected the sanction procedure within the employee handbook to determine that an employee sanction procedure was documented within the employee handbook and communicated that an employee could face disciplinary action, including termination of employment, for noncompliance with a policy and/or procedure.	No exceptions noted.
Communication and Information			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Documented policies, procedures, and network diagrams are in place that identify information required to support the functioning of internal control and achievement of objectives.	Inspected the security policies and procedures and network diagrams to determine that documented policies, procedures, and network diagrams were in place that identified information required to support the functioning of internal control and achievement of objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.2	Security monitoring applications are in place to monitor and analyze the in-scope systems for production image and web vulnerabilities, including any possible or actual security breaches. Identified security vulnerabilities are triaged by the security team and monitored through resolution.	Inspected the security monitoring application configurations, alert configurations, an example alert generated during the period, and a remediation ticket recorded during the period to determine that a security monitoring application was in place to monitor and analyze the in-scope systems for production image and web vulnerabilities, including any possible or actual security breaches, and identified security vulnerabilities were triaged by the security team and monitored through resolution.	No exceptions noted.
CC2.1.3	Vulnerability assessments of in-scope systems are performed on a continuous basis to identify threats and assess their potential impact to system security. Identified security findings classified as critical are triaged by the security team and monitored through resolution.	Inspected the remediation documentation for a sample of critical findings identified during the period to determine that vulnerability assessments of in-scope systems were performed, and security findings were triaged by the security team and monitored through resolution.	No exceptions noted.
CC2.1.4	A third-party specialist performs an annual penetration test. Management reviews the results of the penetration tests and remediation plans are proposed and monitored through resolution.	Inspected the most recent penetration test report, evidence of management review of test results, and remediation plans to determine that a third-party specialist performed a penetration test during the period, management reviewed the results of the penetration test, and remediation plans were proposed and monitored through resolution.	No exceptions noted.
CC2.1.5	Internal audits are performed annually to identify potential control gaps and weaknesses.	Inspected the most recent internal audit results to determine that internal audits were performed during the period to identify potential control gaps and weaknesses.	No exceptions noted.
CC2.1.6	Communication channels are in place to enable external parties to report security incidents, concerns, and complaints.	Inspected the communication channels available and evidence of external party communication notifications received during the period to determine that communication channels were in place to enable external parties to report security incidents, concerns, and complaints.	No exceptions noted.
CC2.1.7	Security personnel monitor the security impact of emerging technologies and the impact of applicable laws or regulations.	Inspected evidence of the security team monitoring security subscriptions to determine that security personnel monitored the security impact of emerging technologies and the impact of applicable laws or regulations.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Documented policies and procedures are in place to guide personnel in areas including, but not limited to, the following: • Information Security • Data retention and destruction • Logical access • Change management	Inspected the security and change management policies and procedures to determine that documented policies and procedures were in place to guide personnel in the following areas: • Information security • Data retention and destruction • Logical access • Change management	No exceptions noted.
CC2.2.2	Internal control responsibilities regarding security are documented within the information security policies. Employees are required to acknowledge that they have read and understand their responsibilities upon hire and annually thereafter.	Inspected the information security policies and the policy acknowledgement for a sample of employees hired during the period to determine that internal control responsibilities regarding security were documented within the information security policies and that each employee sampled acknowledged the policies upon hire.	No exceptions noted.
		Inspected the information security policies and the policy acknowledgement for a sample of current employees to determine that internal control responsibilities regarding security were documented within the information security policies and that each employee sampled acknowledged the policies during the period.	No exceptions noted.
CC2.2.3	Employees are required to complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate security policies.	Inspected security awareness training completion records for a sample of employees hired during the period to determine that each employee sampled completed security awareness training upon hire.	No exceptions noted.
		Inspected security awareness training completion records for a sample of current employees to determine that each employee sampled completed security awareness training during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.4	Documented job descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs, and are communicated to employees through the Discourse intranet.	Inspected the job descriptions for a sample of current employees and evidence of communication of job descriptions via the Discourse intranet to determine that documented job descriptions were in place for each employee sampled to define the skills, responsibilities, and knowledge levels required for particular jobs, and were communicated to employees through the Discourse intranet.	No exceptions noted.
CC2.2.5	Documented escalation procedures for reporting security incidents are provided to internal users to guide them in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the incident response policy to determine that documented escalation procedures for reporting security incidents were provided to internal users to guide them in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC2.2.6	Employees are required to acknowledge, upon hire and at least annually thereafter, that they have been given access to the employee handbook and code of conduct and understand their responsibility for adhering to Discourse's behavioral standards.	Inspected the employee handbook acknowledgement for a sample of employees hired during the period to determine that each employee sampled acknowledged the employee handbook upon hire.	No exceptions noted.
		Inspected the employee handbook acknowledgement for a sample of current employees to determine that each employee sampled acknowledged the employee handbook during the period.	No exceptions noted.
CC2.2.7	Executive management meetings are held with operational management at least annually to discuss and align internal control responsibilities, performance measures, and incentives with company objectives.	Inspected the most recent executive management agenda to determine that executive management meetings were held with operational management during the period to discuss and align internal control responsibilities, performance measures, and incentives with company objectives.	No exceptions noted.
CC2.2.8	Reporting procedures are in place to facilitate the reporting of complaints, unethical behaviors, and fraudulent activities.	Inspected the reporting procedures within the employee handbook to determine that reporting procedures were in place to facilitate the reporting of complaints, unethical behaviors, and fraudulent activities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Discourse's security commitments and the associated system requirements are documented in the enterprise hosting terms.	Inspected the enterprise hosting terms agreement to determine that security commitments and the associated system requirements were documented in the enterprise hosting terms.	No exceptions noted.
CC2.3.2	System components, planned outages, and known issues are communicated to external parties via the company website.	Inquired of the COO regarding external communication to determine that system components, planned outages, and known issues were communicated to external parties via the company website.	No exceptions noted.
		Inspected the Discourse status page to determine that system components, planned outages, and known issues were communicated to external parties via the company website.	No exceptions noted.
CC2.3.3	Vendors and third parties are required to enter an agreement with CDCK for services provided that includes statements of confidentiality.	Inspected the vendor agreement for a sample of vendors to determine that a vendor agreement including statements of confidentiality were executed for each vendor sampled.	No exceptions noted.
CC2.3.4	Documented escalation procedures for reporting security incidents are provided to internal users to guide them in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the incident response policy to determine that documented escalation procedures for reporting security incidents were provided to internal users to guide them in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC2.3.5	Communication channels are in place to enable external parties to report security incidents, concerns, and complaints.	Inspected the communication channels available and evidence of external party communication notifications received during the period to determine that communication channels were in place to enable external parties to report security incidents, concerns, and complaints.	No exceptions noted.
CC2.3.6	Discourse contact information and relevant communication channels are available to external parties via the public-facing website.	Inspected the contact information available to external parties to determine that Discourse contact information and relevant communication channels were available to external parties via the public-facing website.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Risk Assessment			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Information security objectives are formally documented and reviewed by executive management annually to help ensure alignment of internal control responsibilities, performance measures, and incentives with company business objectives.	Inspected the ISMS policy to determine that information security objectives were formally documented and reviewed by executive management during the period to ensure alignment of internal control responsibilities, performance measures, and incentives with company business objectives.	No exceptions noted.
CC3.1.2	Documented policies and procedures are in place to guide personnel in performing the annual risk assessment that include the risk scoring methodology and risk tolerance levels.	Inspected the risk assessment policy and procedures to determine that documented policies and procedures were in place to guide personnel in performing the annual risk assessment that included the risk scoring methodology and risk tolerance levels.	No exceptions noted.
CC3.1.3	Executive management establishes KPIs for operational and internal control effectiveness, including the acceptable level of control operation and failure.	Inspected the risk assessment policy and most recently completed risk assessment to determine that executive management established KPIs for operational and internal control effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk assessment policy and procedures to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
CC3.2.2	A risk assessment is performed annually that considers the identification and assessment of risks relating to the documented objectives. Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review and approval.	Inspected the most recently completed risk assessment to determine that a risk assessment was performed during the period and approved by management. Additionally, determined that the risk assessment considered the identification and assessment of risks relating to the documented objectives and that identified risks were rated using a risk evaluation process with mitigation strategies, as applicable.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.3	Developments in technology and the impact of applicable laws or regulations are considered by a member of the legal team as part of the annual compliance review.	Inspected the compliance review completed during the period to determine that developments in technology and the impact of applicable laws or regulations were considered by a member of the legal team as part of the annual compliance review.	No exceptions noted.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Documented policies and procedures are in place to guide personnel in identifying the potential for fraud when performing the risk assessment process.	Inspected the risk assessment policy and procedures to determine that documented policies and procedures were in place to guide personnel in identifying the potential for fraud when performing the risk assessment process.	No exceptions noted.
CC3.3.2	A risk assessment is performed annually that considers the potential for fraud. Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review and approval.	Inspected the most recently completed risk assessment to determine that a risk assessment was performed during the period and approved by management. Additionally, determined that the risk assessment considered the potential for fraud and that identified risks were rated using a risk evaluation process with mitigation strategies, as applicable.	No exceptions noted.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	Developments in technology and the impact of applicable laws or regulations are considered by executive management as part of the annual risk assessment.	Inspected the most recently completed risk assessment to determine that developments in technology and the impact of applicable laws or regulations were considered by executive management during the period as part of the annual risk assessment.	No exceptions noted.
CC3.4.2	A risk assessment is performed annually that assesses potential system changes. Identified risks are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review and approval.	Inspected the most recently completed risk assessment to determine that a risk assessment was performed during the period and approved by management. Additionally, determined that the risk assessed included potential system changes and that identified risks were rated using a risk evaluation process with mitigation strategies, as applicable.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4.3	ISMC meetings are held with executive management quarterly to discuss and align internal control responsibilities, performance measures, and incentives with company objectives.	Inspected the ISMC meeting agenda for a sample of quarters during the period to determine that ISMC meetings were held with executive management to discuss and align internal control responsibilities, performance measures, and incentives with company objectives for each quarter sampled.	No exceptions noted.
Monitoring Activities			
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Vulnerability assessments of in-scope systems are performed on a continuous basis to identify threats and assess their potential impact to system security. Identified security findings classified as critical are triaged by the security team and monitored through resolution.	Inspected the remediation documentation for a sample of critical findings identified during the period to determine that vulnerability assessments of in-scope systems were performed, and security findings were triaged by the security team and monitored through resolution.	No exceptions noted.
CC4.1.2	A third-party specialist performs an annual penetration test. Management reviews the results of the penetration tests and remediation plans are proposed and monitored through resolution.	Inspected the most recent penetration test report, evidence of management review of test results, and remediation plans to determine that a third-party specialist performed a penetration test during the period, management reviewed the results of the penetration test, and remediation plans were proposed and monitored through resolution.	No exceptions noted.
CC4.1.3	Internal audits are performed annually to identify potential control gaps and weaknesses.	Inspected the most recent internal audit results to determine that internal audits were performed during the period to identify potential control gaps and weaknesses.	No exceptions noted.
CC4.1.4	Results of third-party audits are reviewed by management at least annually.	Inspected the most recent management review of audit reports to determine that results of third-party audits were reviewed by management during the period.	No exceptions noted.
CC4.1.5	The compliance team evaluates vendor risk and reviews vendor compliance reports annually for vendors classified as high risk to help ensure that third-party vendors comply with CDCK's security requirements.	Inspected the vendor risk and compliance evaluation for a sample of vendors classified as high risk to determine that the compliance team evaluated vendor risk and reviewed vendor compliance reports during the period for each vendor sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.6	Security monitoring applications are in place to monitor and analyze the in-scope systems for production image and web vulnerabilities, including any possible or actual security breaches. Identified security vulnerabilities are triaged by the security team and monitored through resolution.	Inspected the security monitoring application configurations, alert configurations, an example alert generated during the period, and a remediation ticket recorded during the period to determine that a security monitoring application was in place to monitor and analyze the in-scope systems for production image and web vulnerabilities, including any possible or actual security breaches, and identified security vulnerabilities were triaged by the security team and monitored through resolution.	No exceptions noted.
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	Internal audits are performed annually to identify potential control gaps and weaknesses.	Inspected the most recent internal audit results to determine that internal audits were performed during the period to identify potential control gaps and weaknesses.	No exceptions noted.
CC4.2.2	Vulnerability assessments of in-scope systems are performed on a continuous basis to identify threats and assess their potential impact to system security. Identified security findings classified as critical are triaged by the security team and monitored through resolution.	Inspected the remediation documentation for a sample of critical findings identified during the period to determine that vulnerability assessments of in-scope systems were performed, and security findings were triaged by the security team and monitored through resolution.	No exceptions noted.
CC4.2.3	A third-party specialist performs an annual penetration test. Management reviews the results of the penetration tests and remediation plans are proposed and monitored through resolution.	Inspected the most recent penetration test report, evidence of management review of test results, and remediation plans to determine that a third-party specialist performed a penetration test during the period, management reviewed the results of the penetration test, and remediation plans were proposed and monitored through resolution.	No exceptions noted.
CC4.2.4	Results of third-party audits are reviewed by management at least annually.	Inspected the most recent management review of audit reports to determine that results of third-party audits were reviewed by management during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.5	ISMC meetings are held with executive management quarterly to discuss and align internal control responsibilities, performance measures, and incentives with company objectives.	Inspected the ISMC meeting agenda for a sample of quarters during the period to determine that ISMC meetings were held with executive management to discuss and align internal control responsibilities, performance measures, and incentives with company objectives for each quarter sampled.	No exceptions noted.
CC4.2.6	The Discourse application is utilized as a ticketing system to document security incidents, response, and resolution.	Inspected the ticket for a sample of security incidents identified during the period to determine that the Discourse application was utilized as a ticketing system to document security incidents, response, and resolution for each security incident sampled.	No exceptions noted.
Control Activities			
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	Documented policies and procedures are in place to guide personnel in performing the risk assessment process that include the development of risk treatment plans to mitigate identified risks.	Inspected the risk assessment policy and procedures to determine that documented policies and procedures were in place to guide personnel in performing the risk assessment process that included the development of risk treatment plans to mitigate identified risks.	No exceptions noted.
CC5.1.2	A risk assessment is performed annually that considers the identification and assessment of risks relating to the documented objectives. Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review and approval.	Inspected the most recently completed risk assessment to determine that a risk assessment was performed during the period and approved by management. Additionally, determined that the risk assessment considered the identification and assessment of risks relating to the documented objectives and that identified risks were rated using a risk evaluation process with mitigation strategies, as applicable.	No exceptions noted.
CC5.1.3	Assigned risk owners select and develop risk response actions to mitigate the risks identified during the annual risk assessment process. Risk owners document the response actions within risk registers for risks above the tolerable threshold.	Inspected the most recently completed risk assessment to determine that assigned risk owners selected and developed risk response actions, as applicable, during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Assigned risk owners select and develop risk response actions over technology to support the achievement of objectives as an output from the annual risk assessment process. Risk owners document the response actions within risk registers for risks above the tolerable threshold.	Inspected the most recently completed risk assessment to determine that assigned risk owners selected and developed risk response actions over technology, as applicable, during the period.	No exceptions noted.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Documented policies and procedures are in place to guide personnel in areas including, but not limited to, the following: • Information Security • Data retention and destruction • Logical access • Change management	Inspected the security and change management policies and procedures to determine that documented policies and procedures were in place to guide personnel in the following areas: • Information security • Data retention and destruction • Logical access • Change management	No exceptions noted.
CC5.3.2	Employees are required to acknowledge, upon hire and at least annually thereafter, that they have been given access to the employee handbook and code of conduct and understand their responsibility for adhering to Discourse's behavioral standards.	Inspected the employee handbook acknowledgement for a sample of employees hired during the period to determine that each employee sampled acknowledged the employee handbook upon hire.	No exceptions noted.
		Inspected the employee handbook acknowledgement for a sample of current employees to determine that each employee sampled acknowledged the employee handbook during the period.	No exceptions noted.
CC5.3.3	Internal control responsibilities regarding security are documented within the information security policies. Employees are required to acknowledge that they have read and understand their responsibilities upon hire and annually thereafter.	Inspected the information security policies and the policy acknowledgement for a sample of employees hired during the period to determine that internal control responsibilities regarding security were documented within the information security policies and that each employee sampled acknowledged the policies upon hire.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the information security policies and the policy acknowledgement for a sample of current employees to determine that internal control responsibilities regarding security were documented within the information security policies and that each employee sampled acknowledged the policies during the period.	No exceptions noted.
CC5.3.4	An employee sanction procedure is documented within the employee handbook communicating that an employee could face disciplinary action, including termination of employment, for noncompliance with a policy and/or procedure.	Inspected the sanction procedure within the employee handbook to determine that an employee sanction procedure was documented within the employee handbook and communicated that an employee could face disciplinary action, including termination of employment, for noncompliance with a policy and/or procedure.	No exceptions noted.
Logical and Physical Access Controls			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	Documented policies and procedures are in place to guide personnel in CDCK's requirements for implementing and maintaining logical access controls to information assets, including: • "Need to Know" Access Principles • User Access Provisioning / Deprovisioning • Shared Account Restrictions • Account Logging and Monitoring	Inspected the access control policy to determine that policies and procedures were in place to guide personnel in CDCK's requirements for implementing and maintaining logical access controls to information assets, including: • "Need to Know" Access Principles • User Access Provisioning / Deprovisioning • Shared Account Restrictions • Account Logging and Monitoring	No exceptions noted.
CC6.1.2	Documented standard build procedures and images are utilized for the installation of production infrastructure.	Inspected the standard build procedures and images to determine that documented standard build procedures and images were utilized for the installation of production infrastructure.	No exceptions noted.
CC6.1.3	The in-scope systems are configured to authenticate users with a unique user account and enforce minimum password requirements or SSH public key authentication.	Inspected the in-scope system authentication configurations and user listings to determine that the in-scope systems were configured to authenticate users with a unique user account and enforce minimum password requirements or SSH public key authentication.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.4	CDCK employees authenticate via a user account, password, and MFA before being granted access to the Discourse application.	Inspected the Discourse application authentication configurations to determine that CDCK employees were required to authenticate via a user account, password, and MFA before being granted access to the Discourse application.	No exceptions noted.
CC6.1.5	Predefined user access groups are utilized to assign role-based access privileges and segregate access to data within the in-scope systems.	Inspected the in-scope system user listings to determine that predefined user access groups were utilized to assign role-based access privileges and segregate access to data within the in-scope systems.	No exceptions noted.
CC6.1.6	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized engineering and development personnel.	Inspected the listing of administrator accounts for the in-scope systems with the assistance of the company cofounders to determine that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized engineering and development personnel.	No exceptions noted.
CC6.1.7	Passwords are stored in an encrypted format.	Inspected the password encryption configurations to determine that passwords were stored in an encrypted format.	No exceptions noted.
CC6.1.8	Firewalls are in place to filter unauthorized inbound network traffic from the Internet and are configured to deny any type of network connection that is not explicitly authorized by a rule.	Inspected the firewall ruleset / access control list to determine that firewalls were in place to filter unauthorized inbound network traffic from the Internet and configured to deny any type of network connection that was not explicitly authorized by a rule.	No exceptions noted.
	AWS is responsible for implementing controls that ensure logical access to the underlying network and virtualization management software is managed for its cloud hosting services where in-scope systems reside.		
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	Documented policies are in place to guide personnel in the provisioning, modification, and revocation of user access permissions, and the periodic access revalidation processes.	Inspected the logical access policies to determine that documented policies were in place to guide personnel in the provisioning, modification, and revocation of user access permissions, and the periodic access revalidation processes.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.2	User access requests are documented and require manager approval.	Inspected the user access request form for a sample of user access requests to in-scope systems received and processed during the period to determine that each access request sampled was documented and approved by a manager.	No exceptions noted.
CC6.2.3	Revocation requests are completed, and access is revoked for employees as a component of the termination process.	Inspected the termination form for a sample of employees terminated during the period to determine that revocation requests were completed for each employee sampled.	No exceptions noted.
		Inspected the listing of users with access to in-scope systems for a sample of employees terminated during the period to determine that the sampled employees did not retain active accounts.	No exceptions noted.
CC6.2.4	Infrastructure personnel perform quarterly user access reviews, including a review of privileged users, to help ensure that access is restricted to authorized personnel.	Inspected the completed user access review for a sample of quarters during the period to determine that user access reviews, including privileged users, were performed for each quarter sampled.	No exceptions noted.
	AWS is responsible for implementing controls that ensure logical access to the underlying network and virtualization management software is managed for its cloud hosting services where in-scope systems reside.		
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	User access requests are documented and require manager approval.	Inspected the user access request form for a sample of user access requests to in-scope systems received and processed during the period to determine that each access request sampled was documented and approved by a manager.	No exceptions noted.
CC6.3.2	Revocation requests are completed, and access is revoked for employees as a component of the termination process.	Inspected the termination form for a sample of employees terminated during the period to determine that revocation requests were completed for each employee sampled.	No exceptions noted.
		Inspected the listing of users with access to in-scope systems for a sample of employees terminated during the period to determine that the sampled employees did not retain active accounts.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.3	Predefined user access groups are utilized to assign role-based access privileges and segregate access to data within the in-scope systems.	Inspected the in-scope system user listings to determine that predefined user access groups were utilized to assign role-based access privileges and segregate access to data within the in-scope systems.	No exceptions noted.
CC6.3.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized engineering and development personnel.	Inspected the listing of administrator accounts for the in-scope systems with the assistance of the company cofounders to determine that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized engineering and development personnel.	No exceptions noted.
CC6.3.5	Infrastructure personnel perform quarterly user access reviews, including a review of privileged users, to help ensure that access is restricted to authorized personnel.	Inspected the completed user access review for a sample of quarters during the period to determine that user access reviews, including privileged users, were performed for each quarter sampled.	No exceptions noted.
	AWS is responsible for implementing controls that ensure logical access to the underlying network and virtualization management software is managed for its cloud hosting services where in-scope systems reside.		
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.			
CC6.4.1	CDCK maintains a listing of individuals authorized to access the in-scope data center facilities.	Inspected the data center access listings to determine that CDCK maintained a listing of individuals authorized to access the HE and Equinix data center facilities.	No exceptions noted.
CC6.4.2	Infrastructure personnel perform quarterly physical access reviews to help ensure that access to in-scope data center facilities is restricted to authorized personnel.	Inspected the user access review for a sample of quarters during the period to determine that physical access reviews were performed for each quarter sampled.	No exceptions noted.
	HE, Equinix, and AWS are responsible for implementing controls that ensure physical access to facilities and system components including firewalls, routers, and servers is restricted to authorized personnel.		
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	Documented information classification, handling, and disposal policies are in place to guide personnel in the categorization of information and the handling and disposal or destruction of data.	Inspected the retention and destruction policy to determine that documented information classification, handling, and disposal policies were in place to guide personnel in the categorization of information and the handling and disposal or destruction of data.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.5.2	CDCK maintains a listing of individuals authorized to access the in-scope data center facilities.	Inspected the data center access listings to determine that CDCK maintained a listing of individuals authorized to access the HE and Equinix data center facilities.	No exceptions noted.
	AWS is responsible for implementing controls that ensure logical access to the underlying network and virtualization management software is managed for its cloud hosting services where in-scope systems reside.		
	HE, Equinix, and AWS are responsible for implementing controls that ensure physical access to facilities and system components including firewalls, routers, and servers is restricted to authorized personnel.		
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Firewalls are in place to filter unauthorized inbound network traffic from the Internet and are configured to deny any type of network connection that is not explicitly authorized by a rule.	Inspected the firewall ruleset / access control list to determine that firewalls were in place to filter unauthorized inbound network traffic from the Internet and configured to deny any type of network connection that was not explicitly authorized by a rule.	No exceptions noted.
CC6.6.2	Web servers utilize TLS encryption for web communication sessions.	Inspected the web server certificate and encryption details to determine that web servers utilized TLS encryption for web communication sessions.	No exceptions noted.
	AWS is responsible for implementing controls that ensure logical access to the underlying network and virtualization management software is managed for its cloud hosting services where in-scope systems reside.		
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Policies are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	Inspected the encryption policy to determine that policies were in place that prohibited the transmission of sensitive information over the Internet or other public communications paths unless it was encrypted.	No exceptions noted.
CC6.7.2	Web servers utilize TLS encryption for web communication sessions.	Inspected the web server certificate and encryption details to determine that web servers utilized TLS encryption for web communication sessions.	No exceptions noted.
CC6.7.3	Policies are in place that prohibit the use of removable media unless it is encrypted.	Inspected the removable media policy to determine that policies were in place that prohibited the use of removable media unless it was encrypted.	No exceptions noted.
CC6.7.4	Data at rest is protected using full disk encryption.	Inspected the disk encryption configurations to determine that data at rest was protected using full disk encryption.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	Endpoint security software is utilized to centrally manage antivirus and security updates for workstations.	Inspected the endpoint security software antivirus and security update configurations to determine that endpoint security software was utilized to centrally manage antivirus and security updates for workstations.	No exceptions noted.
CC6.8.2	The ability to implement changes to in-scope systems is restricted to user accounts accessible by authorized personnel who do not have code development responsibilities.	Inspected the listing of personnel with the ability to implement changes to in-scope systems to determine that the ability to implement changes to in-scope systems was restricted to user accounts accessible by authorized personnel who do not have code development responsibilities.	No exceptions noted.
CC6.8.3	Security monitoring applications are in place to monitor and analyze the in-scope systems for production image and web vulnerabilities, including any possible or actual security breaches. Identified security vulnerabilities are triaged by the security team and monitored through resolution.	Inspected the security monitoring application configurations, alert configurations, an example alert generated during the period, and a remediation ticket recorded during the period to determine that a security monitoring application was in place to monitor and analyze the in-scope systems for production image and web vulnerabilities, including any possible or actual security breaches, and identified security vulnerabilities were triaged by the security team and monitored through resolution.	No exceptions noted.
System Operations			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	Documented policies and procedures are in place to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems.	Inspected the security and change management policies and procedures to determine that documented policies and procedures were in place to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.2	Security monitoring applications are in place to monitor and analyze the in-scope systems for production image and web vulnerabilities, including any possible or actual security breaches. Identified security vulnerabilities are triaged by the security team and monitored through resolution.	Inspected the security monitoring application configurations, alert configurations, an example alert generated during the period, and a remediation ticket recorded during the period to determine that a security monitoring application was in place to monitor and analyze the in-scope systems for production image and web vulnerabilities, including any possible or actual security breaches, and identified security vulnerabilities were triaged by the security team and monitored through resolution.	No exceptions noted.
CC7.1.3	Vulnerability assessments of in-scope systems are performed on a continuous basis to identify threats and assess their potential impact to system security. Identified security findings classified as critical are triaged by the security team and monitored through resolution.	Inspected the remediation documentation for a sample of critical findings identified during the period to determine that vulnerability assessments of in-scope systems were performed, and security findings were triaged by the security team and monitored through resolution.	No exceptions noted.
CC7.1.4	A third-party specialist performs an annual penetration test. Management reviews the results of the penetration tests and remediation plans are proposed and monitored through resolution.	Inspected the most recent penetration test report, evidence of management review of test results, and remediation plans to determine that a third-party specialist performed a penetration test during the period, management reviewed the results of the penetration test, and remediation plans were proposed and monitored through resolution.	No exceptions noted.
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	Documented escalation procedures for reporting security incidents are provided to internal users to guide them in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the incident response policy to determine that documented escalation procedures for reporting security incidents were provided to internal users to guide them in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.2	Security monitoring applications are in place to monitor and analyze the in-scope systems for production image and web vulnerabilities, including any possible or actual security breaches. Identified security vulnerabilities are triaged by the security team and monitored through resolution.	Inspected the security monitoring application configurations, alert configurations, an example alert generated during the period, and a remediation ticket recorded during the period to determine that a security monitoring application was in place to monitor and analyze the in-scope systems for production image and web vulnerabilities, including any possible or actual security breaches, and identified security vulnerabilities were triaged by the security team and monitored through resolution.	No exceptions noted.
CC7.2.3	Vulnerability assessments of in-scope systems are performed on a continuous basis to identify threats and assess their potential impact to system security. Identified security findings classified as critical are triaged by the security team and monitored through resolution.	Inspected the remediation documentation for a sample of critical findings identified during the period to determine that vulnerability assessments of in-scope systems were performed, and security findings were triaged by the security team and monitored through resolution.	No exceptions noted.
CC7.2.4	A third-party specialist performs an annual penetration test. Management reviews the results of the penetration tests and remediation plans are proposed and monitored through resolution.	Inspected the most recent penetration test report, evidence of management review of test results, and remediation plans to determine that a third-party specialist performed a penetration test during the period, management reviewed the results of the penetration test, and remediation plans were proposed and monitored through resolution.	No exceptions noted.
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	Documented escalation procedures for reporting security incidents are provided to internal users to guide them in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the incident response policy to determine that documented escalation procedures for reporting security incidents were provided to internal users to guide them in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC7.3.2	Postmortem evaluations are completed for security incidents classified as critical to help ensure corrective measures are implemented.	Inspected the postmortem evaluation for a sample of critical security incidents that required postmortem evaluations during the period to determine that postmortem evaluations were completed for each sampled security incident classified as critical.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3.3	The Discourse application is utilized as a ticketing system to document security incidents, response, and resolution.	Inspected the ticket for a sample of security incidents identified during the period to determine that the Discourse application was utilized as a ticketing system to document security incidents, response, and resolution for each security incident sampled.	No exceptions noted.
CC7.3.4	Incidents requiring a change to the system follow the standard change control process.	Inquired of the technical advocate regarding incident management to determine that incidents that required a change to the system followed the standard change control process.	No exceptions noted.
		Inspected the change ticket for an example incident requiring a change to the system during the period to determine that incidents requiring a change to the system followed the standard change control process.	No exceptions noted.
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	Documented escalation procedures for reporting security incidents are provided to internal users to guide them in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the incident response policy to determine that documented escalation procedures for reporting security incidents were provided to internal users to guide them in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC7.4.2	Employee roles and responsibilities are documented within the incident response policy and procedures.	Inspected the incident response policy and procedures to determine that employee roles and responsibilities were documented within the incident response policy and procedures.	No exceptions noted.
CC7.4.3	Postmortem evaluations are completed for security incidents classified as critical to help ensure corrective measures are implemented.	Inspected the postmortem evaluation for a sample of critical security incidents that required postmortem evaluations during the period to determine that postmortem evaluations were completed for each sampled security incident classified as critical.	No exceptions noted.
CC7.4.4	The Discourse application is utilized as a ticketing system to document security incidents, response, and resolution.	Inspected the ticket for a sample of security incidents identified during the period to determine that the Discourse application was utilized as a ticketing system to document security incidents, response, and resolution for each security incident sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4.5	Incidents requiring a change to the system follow the standard change control process.	Inquired of the technical advocate regarding incident management to determine that incidents that required a change to the system followed the standard change control process.	No exceptions noted.
		Inspected the change ticket for an example incident requiring a change to the system during the period to determine that incidents requiring a change to the system followed the standard change control process.	No exceptions noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Documented escalation procedures for reporting security incidents are provided to internal users to guide them in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the incident response policy to determine that documented escalation procedures for reporting security incidents were provided to internal users to guide them in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC7.5.2	A documented incident response plan is in place and tested annually.	Inspected the incident response plan and the most recently completed incident response plan test to determine that a documented incident response plan was in place and tested during the period.	No exceptions noted.
CC7.5.3	Postmortem evaluations are completed for security incidents classified as critical to help ensure corrective measures are implemented.	Inspected the postmortem evaluation for a sample of critical security incidents that required postmortem evaluations during the period to determine that postmortem evaluations were completed for each sampled security incident classified as critical.	No exceptions noted.
CC7.5.4	The Discourse application is utilized as a ticketing system to document security incidents, response, and resolution.	Inspected the ticket for a sample of security incidents identified during the period to determine that the Discourse application was utilized as a ticketing system to document security incidents, response, and resolution for each security incident sampled.	No exceptions noted.
CC7.5.5	Incidents requiring a change to the system follow the standard change control process.	Inquired of the technical advocate regarding incident management to determine that incidents that required a change to the system followed the standard change control process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the change ticket for an example incident requiring a change to the system during the period to determine that incidents requiring a change to the system followed the standard change control process.	No exceptions noted.
Change Management			
CC8.1 The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Documented change management policies and procedures are in place to guide personnel in the initiation, ownership, responsibilities, and documentation of changes.	Inspected the change management policies and procedures to determine that documented change management policies and procedures were in place to guide personnel in the initiation, ownership, responsibilities, and documentation of changes.	No exceptions noted.
CC8.1.2	Change ticketing systems are in place to document, manage, and monitor application and infrastructure changes from change request through implementation.	Inspected the change documentation for a sample of application and infrastructure changes implemented during the period to determine that each change sampled was documented within the ticketing systems.	No exceptions noted.
CC8.1.3	Changes made to in-scope systems are documented, tested when applicable, and approved prior to implementation.	Inspected the change tickets for a sample of application and infrastructure changes implemented during the period and the version control software branch protection configurations to determine that each change sampled was documented, tested as applicable, and approved prior to implementation.	No exceptions noted.
CC8.1.4	The version control software is configured to enforce code review and approval prior to merging code to the main branch.	Inspected the version control software branch protection configurations to determine that the version control software was configured to enforce code review and approval prior to merging code to the main branch.	No exceptions noted.
CC8.1.5	The production environment is physically and logically segmented from the development and test environments.	Inspected the segmented logical instances and physical separation to determine that the production environment was physically and logically segmented from the development and test environments.	No exceptions noted.
CC8.1.6	Version control software is utilized to provide rollback capabilities and restrict access to application source code to authorized engineering, development, and management personnel.	Inspected the version control software rollback configurations to determine that the version control software was utilized to provide rollback capabilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the user access listing for the version control software to determine that the version control software was utilized to restrict access to application source code to authorized engineering, development, and management personnel.	No exceptions noted.
CC8.1.7	Administrative access privileges within the version control software are restricted to user accounts accessible by authorized engineering and management personnel.	Inspected the listing of users with administrative access within the version control software to determine that administrative access privileges within the version control software were restricted to user accounts accessible by authorized engineering and management personnel.	No exceptions noted.
CC8.1.8	Incidents requiring a change to the system follow the standard change control process.	Inquired of the technical advocate regarding incident management to determine that incidents that required a change to the system followed the standard change control process.	No exceptions noted.
		Inspected the change ticket for an example incident requiring a change to the system during the period to determine that incidents requiring a change to the system followed the standard change control process.	No exceptions noted.
CC8.1.9	The ability to implement changes to in-scope systems is restricted to user accounts accessible by authorized personnel who do not have code development responsibilities.	Inspected the listing of personnel with the ability to implement changes to in-scope systems to determine that the ability to implement changes to in-scope systems was restricted to user accounts accessible by authorized personnel who do not have code development responsibilities.	No exceptions noted.
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk assessment policy and procedures to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.2	A risk assessment is performed annually that considers risks arising from potential business disruptions. Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review and approval.	Inspected the most recently completed risk assessment to determine that a risk assessment was performed during the period and approved by management. Additionally, determined that the risk assessment considered risks arising from potential business disruptions and that identified risks were rated using a risk evaluation process with mitigation strategies, as applicable.	No exceptions noted.
CC9.1.3	Assigned risk owners select and develop risk response actions to mitigate the risks identified during the annual risk assessment process. Risk owners document the response actions within risk registers for risks above the tolerable threshold.	Inspected the most recently completed risk assessment to determine that assigned risk owners selected and developed risk response actions, as applicable, during the period.	No exceptions noted.
CC9.1.4	A business continuity plan and disaster recovery plan are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inspected the business continuity plan and disaster recovery plan to determine that a business continuity plan and disaster recovery plan were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
CC9.1.5	Risk mitigation activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of CDCK to meet its objectives.	Inspected the current cyber insurance policy and the risk assessment policy and procedures to determine that risk mitigation activities considered the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of CDCK to meet its objectives.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Policies and procedures are in place to guide personnel in the identification, monitoring, and audit of third-party providers.	Inspected the vendor management policy to determine that policies and procedures were in place to guide personnel in the identification, monitoring, and audit of third-party providers.	No exceptions noted.
CC9.2.2	Risks arising from the use of vendors providing goods and services are analyzed as part of the annual risk assessment.	Inspected the most recently completed risk assessment to determine that risks arising from the use of vendors providing goods and services were analyzed as part of the annual risk assessment performed during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2.3	The compliance team evaluates vendor risk and reviews vendor compliance reports annually for vendors classified as high risk to help ensure that third-party vendors comply with CDCK's security requirements.	Inspected the vendor risk and compliance evaluation for a sample of vendors classified as high risk to determine that the compliance team evaluated vendor risk and reviewed vendor compliance reports during the period for each vendor sampled.	No exceptions noted.
CC9.2.4	Vendors and third parties are required to enter an agreement with CDCK for services provided that includes statements of confidentiality.	Inspected the vendor agreement for a sample of vendors to determine that a vendor agreement including statements of confidentiality were executed for each vendor sampled.	No exceptions noted.