

CLOUDFLARE, INC.

SOC 2 REPORT

FOR

AREA 1 SECURITY SOLUTION

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS
RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

JANUARY 1, 2023, TO MARCH 31, 2023

Attestation and Compliance Services



Proprietary & Confidential

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

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

If the 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.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1	INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2	MANAGEMENT'S ASSERTION	5
SECTION 3	DESCRIPTION OF THE SYSTEM	7
SECTION 4	TESTING MATRICES	20

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Cloudflare, Inc.:

Scope

We have examined Cloudflare, Inc.'s ("Cloudflare" or the "service organization") accompanying description of its Area 1 Security Solution system, in Section 3, throughout the period January 1, 2023, to March 31, 2023, (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 January 1, 2023, to March 31, 2023, to provide reasonable assurance that Cloudflare's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Cloudflare uses various subservice organizations for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Cloudflare, to achieve Cloudflare's service commitments and system requirements based on the applicable trust services criteria. The description presents Cloudflare's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Cloudflare'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

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

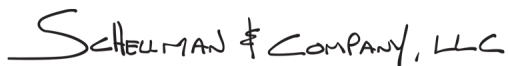
- a. the description presents Cloudflare's Area 1 Security Solution system that was designed and implemented throughout the period January 1, 2023, to March 31, 2023, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period January 1, 2023, to March 31, 2023, to provide reasonable assurance that Cloudflare'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 Cloudflare's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period January 1, 2023, to March 31, 2023, to provide reasonable assurance that Cloudflare'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 Cloudflare'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 Cloudflare; user entities of Cloudflare's Area 1 Security Solution system during some or all of the period of January 1, 2023, to March 31, 2023, business partners of Cloudflare subject to risks arising from interactions with the Area 1 Security Solution 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.

Scheelman & Company, LLC

Tampa, Florida
May 22, 2023

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Cloudflare's Area 1 Security Solution system, in Section 3, throughout the period January 1, 2023, to March 31, 2023, (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 Area 1 Security Solution system that may be useful when assessing the risks arising from interactions with Cloudflare's system, particularly information about system controls that Cloudflare has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Cloudflare uses various subservice organizations for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Cloudflare, to achieve Cloudflare's service commitments and system requirements based on the applicable trust services criteria. The description presents Cloudflare's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Cloudflare'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 Cloudflare's Area 1 Security Solution system that was designed and implemented throughout the period January 1, 2023, to March 31, 2023, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period January 1, 2023, to March 31, 2023, to provide reasonable assurance that Cloudflare'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 Cloudflare's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period January 1, 2023, to March 31, 2023, to provide reasonable assurance that Cloudflare'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 Cloudflare's controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Cloudflare, Inc. (Cloudflare) was founded in 2009 with the core mission of helping to build a better Internet. Cloudflare is a cloud-based company that provides security, performance, and reliability services, such as a Content Delivery Network (CDN) solution, distributed denial-of-service (DDoS) mitigation, Domain Name System (DNS), Web Application Firewall (WAF). Cloudflare also provides customers with paid enhancements that customers can utilize to increase the level of their website's security, performance, and reliability. Cloudflare's technology is hosted on cloud computing infrastructure and the product dashboard can be accessed from any web browser.

Description of Services Provided

Cloudflare Area 1 is a cloud-native e-mail security service that identifies and blocks attacks before they hit user inboxes, enabling more effective protection against spear phishing, Business E-mail Compromise (BEC), and other advanced threats that evade existing defenses. Area 1 enhances built-in security from cloud e-mail providers with deep integrations into Microsoft and Google environments and workflows. Area 1 is part of the Cloudflare Zero Trust platform that helps increase visibility, eliminate complexity, and reduce for remote and office users.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Cloudflare designs its processes and procedures related to the Area 1 Security Solution system to meet its objectives. Those objectives are based on the service commitments that Cloudflare makes to user entities; the laws and regulations that govern the provision of the Area 1 Security Solution system; and the financial, operational, and compliance requirements that Cloudflare has established for the service. The Area 1 Security Solution system is subject to the relevant regulatory and industry information and data security requirements in which Cloudflare operates.

Security, availability, and confidentiality commitments to user entities are documented and communicated in the security exhibit and enterprise subscription terms of service located on the Cloudflare website. The principal security, availability, and confidentiality commitments are standardized and include the following:

- Implement and maintain a comprehensive written information security program.
- Provide and deliver information security awareness training to Cloudflare employees at the time of hire.
- Perform continuous monitoring, logging, and relevant alerting for security events.
- Protect the information system from unauthorized access, use, modification, disclosure, destruction, threats, or hazards.
- Maintain a third-party risk management program.
- Conduct regular security assessments of Cloudflare's infrastructure and applications.
- Security and hardening standards for servers and network devices, based on industry best practices are implemented and maintained.
- Apply security patches and system updates to Cloudflare-managed software and applications, appliances, and operating systems according to industry standards.
- Follow secure software development life cycle (SDLC) secure coding practices.
- Encrypt customer data at rest and in transit.
- Maintain and exercise a disaster recovery plan to ensure recovery in the event of a business disruption.

- Maintain and annually update a documented data breach action and response plan.
- Delete customer data at any time after 72 hours from the time such customer data is captured by Cloudflare, except for any customer account information included therein that is reasonably required for the operation of the services.

Cloudflare establishes system requirements that refer to how the system should function to support the achievement of the principal service commitments, relevant laws and regulations, and guidelines of industry groups. These requirements include, but are not limited to, defined processes around the following:

- The information security program is updated and reviewed at least annually.
- Employees are provided with security awareness training upon hire and annually thereafter.
- Production systems are monitored in accordance with predefined security criteria and alerts are sent to authorized personnel. Confirmed incidents are tracked to resolution.
- Authorized users are required to use two-factor authentication to access systems where customer data resides.
- An employee termination process is in place to remove access upon termination of employment or when access is no longer required.
- User access reviews are performed on a regular basis and inappropriate personnel access is promptly removed.
- Security incidents are confirmed and analyzed for impact by a dedicated security incident response team. Confirmed incidents are classified, prioritized, and logged.
- Quarterly vulnerability scans and annual penetration testing are performed at least annually.
- Mechanisms are utilized to detect deviations from baseline configurations in production environments.
- A device management tool is configured to check employee workstations for security-relevant patches at least daily and install software and/or firmware updates, as applicable.
- Security patches are released automatically to in-scope servers through a configuration system to help ensure current patches are implemented.
- Change management procedures are documented and maintained.
- A tool is configured to scan source code for vulnerabilities.
- Customer data is encrypted at rest and in transit via advanced encryption standard (AES) minimum 256-bit encryption.
- Risk assessment policies and procedures are documented to provide assurance that risks to the achievement of the principal service commitments are identified and mitigated to acceptable levels.
- Third-party attestation reports, security questionnaires, or service provider reported information security controls are reviewed prior to engagement and annually thereafter.
- A disaster recovery plan is in place and tested to help recover from business disruptions.
- Cloudflare maintains an incident response plan that defines the type of incidents that need to be managed, tracked, and reported.
- A data deletion script is configured in the production environment to delete data upon customer request after the expiration of the retention period and in accordance with Cloudflare's internal retention requirements.

Such requirements are communicated in Cloudflare's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed; how the system is operated; how the internal business systems and networks are managed; and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been

documented on how to carry out specific manual and automated processes required in the operation and development of the Area 1 Security Solution system.

In accordance with the 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

The production information systems are located at facilities hosted by Amazon Web Services (AWS) and Google Cloud Platform (GCP). A combination of custom developed, externally supported, and wholly purchased applications supports the Area 1 service.

Primary Infrastructure			
Production Application	Business Function Description	Operating System Platform	Physical Location
Databases	Production databases that hold customer data.	AWS	AWS (US-East-1, US-West-2, EU-Central-1)
Identify Service	Vendor provided secure identity management and single sign-on (SSO).	Okta	AWS (US-East-1, US-West-2, EU-Central-1) GCP (US-Central-1)
Firewall systems	Third-party web-based firewall application in place to filter unauthorized inbound network traffic from the Internet.	AWS & GCP	
Production Servers	Virtual instances that provide scalable computing capacity supporting the system.		

Software	Business Function Description
Cloud-based business productivity tools	Communication and file storage.
Internal project management and developer tools	Planning, tracking, and executing projects, as well as for internal documentation.
Password manager	Generates strong credentials and stores them securely.
Encryption software	Disk and file encryption software.

Software	Business Function Description
Endpoint security software	Anti-malware and anti-virus.
Customer support dashboard	Authenticating and managing electronic agreements.
Monitoring software	Corporate and production network monitoring, alerting and prevention tool; alerting service; automatic attack handling pipeline tool; and aggregation dashboard providing insight into detected attacks.
Source code management software	Application for version control of production and application source code; configuration management software and remote execution engine; and build server application for continuous integration.

People

The following functional areas are used to support the Cloudflare Area 1 Security Solution system:

- Cloudflare Board of Directors – responsible for making objective evaluations and decisions regarding the Company’s mission, vision, and values.
- Cloudflare Security Leadership Team – responsible for coordinating corporate security initiatives at the executive level and enabling Cloudflare to optimize spending, allocate resources, provide oversight, and minimize security risk.
- Security – responsible for direct input into the development and implementation of information security, availability, and confidentiality requirements. Security is comprised of the Security compliance team who are responsible for the oversight of all security compliance requirements and security engineering.
- Product Security – responsible for maintaining and developing secure products.
- Engineering – responsible for the development and delivery of Cloudflare’s internal tools and Area 1. The Engineering team is also composed of site reliability engineers who are responsible for maintenance and monitoring the availability and capacity of the Area 1 service.
- Site Reliability Engineering – responsible for maintaining operational stability across Cloudflare’s Area 1 service.
- Infrastructure – responsible for building, monitoring, and maintaining the global network for Cloudflare.
- IT – responsible for the administration and maintenance of internal Cloudflare systems including providing and revoking system access to employees.
- Customer Support – responsible for solving customer problems, issues, and incidents.
- HR / People Team – responsible for the recruiting and development of Cloudflare employees. Responsibilities include, but are not limited to, maintaining organizational structure, onboarding employees, and offboarding employees.
- Legal – responsible for creating systems and policies that support Cloudflare’s Area 1 service including customer contracts, confidentiality agreements, and internal communication channels.

Procedures

Access, Authentication, and Authorization

User and device authentication to information systems requires a unique username and password that meet Cloudflare’s password complexity requirements and multi-factor authentication is required for remote sessions and access to the production environment. Access to modify source code and access to the cryptographic keystores is limited to authorized personnel and the use of utility programs that might be capable of overriding system and application controls is restricted. To prevent unauthorized changes to customer accounts, Cloudflare employees

are required to obtain enterprise customer authorization to make changes on the customer's behalf. Employees with access to make changes to customer accounts are restricted to authorized personnel.

Access Requests and Access Revocation

Provisioning to information systems and networks is restricted based on default job groups / roles and in accordance with Cloudflare's access control policies and procedures. Approval is required from appropriate personnel for access outside the default job group.

When an employee leaves Cloudflare, it is communicated to leadership, the people team, and the IT department. The people team initiates and communicates terminations or job transfers to the IT department and application owners to remove the terminated user's logical access or modify logical access of employee transfers. Logical access that is no longer required in the event of a termination is documented, communicated to IT, and the user is deactivated, and linked accounts are deprovisioned. Cloudflare performs account and access reviews quarterly and corrective action is taken, when applicable.

Change Management

A Cloudflare SDLC and change management policy is in place to guide employees in making code changes and managing the software / system release procedures for application and configuration changes. Prior to introducing changes into the production environment, review and approval from authorized personnel are required based on the change description, change impact, and test results. Application and infrastructure changes are tracked in a ticketing system. The ability to promote changes to the production environment is restricted to authorized personnel. Changes are designed to have a rollback plan that fails the system to a known state to minimize downtime.

Version control software is utilized for the application change management process and is configured to require independent code review and approval by an individual other than the one who initiated the pull request. Branch protections are enabled to prevent a user from circumventing the approval requirements enforced by the version control software. Access control to configure these branch protections is restricted to authorized personnel that do not have the ability to write code. Additionally, to protect the security of the systems during the change management process, source code is scanned for vulnerabilities prior to implementation.

Data Backup and Disaster Recovery

Cloudflare's Area 1 is designed for high availability and redundancy. Cloudflare configures redundant systems and performs daily backups of databases containing customer and end user data to resume system operation in the event of a system failure. Cloudflare performs backup restoration and failover tests annually to confirm the reliability and integrity of system backups and recovery operations.

Cloudflare identifies the business impact of relevant threats to assets, infrastructure, and resources that support core business functions. Recovery objectives are established for critical business functions. The business continuity and disaster recovery plan is reviewed, approved by management, and communicated to relevant team members annually. Additionally, Cloudflare maintains emergency management documentation which is communicated to employees.

Business contingency and disaster recovery tests are performed annually and Cloudflare management ensures the following:

- Tests are executed with relevant contingency teams
- Test results are documented
- Corrective actions are taken for exceptions noted
- Plans are updated based on test results

System Monitoring

Engineering personnel are responsible for monitoring and supporting the Area 1 service and the security team is responsible for monitoring suspicious user activities.

Security hardening and baseline configuration standards have been established according to industry standards and are reviewed and updated at least annually. Mechanisms are used to detect deviations from baseline configurations in production environments. Cloudflare conducts internal vulnerability scans at least quarterly and penetration tests at least annually. Cloudflare also contracts a third-party ethical hacking company to help identify external vulnerabilities in the form of a bug bounty program. Vulnerabilities identified from the vulnerability scans, penetration tests, bug bounty program are tracked through revolution via the ticketing system.

Production systems are monitored in accordance with predefined security and availability criteria. Cloudflare defines monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts. Cloudflare logs information system activity to a secure repository and restricts the number of administrators with access to audit logs to limited personnel.

Incident Response

Cloudflare maintains an incident response plan that defines the types of incidents that need to be managed, tracked, and reported. Confirmed incidents are assigned a priority level and managed to resolution. Additionally, the incident response team performs a postmortem for incidents classified as P0 or P1. The customer support team also follows established policies and procedures for handling customer-reported incidents.

Data

Cloudflare processes three types of data with respect to their customers:

- When a Cloudflare customer registers for an account, Cloudflare collects contact information. This contact information may include the customer's name, the e-mail address(es) of the account administrator(s), telephone number, and addresses necessary to process payment and delivery of the services. In addition, when customers use the services, Cloudflare collects information about account configurations and the services.
- Cloudflare processes end users' interactions with customer's Internet properties and the services. This information is processed when end users access or use Cloudflare customers' domains, websites, APIs, applications, devices, end points, and networks that use one or more services, and when end users access or use services, such as Cloudflare Zero Trust. The information processed may include, but is not limited to, IP addresses, traffic routing data, system configuration information, and other information about traffic to and from customers' websites, devices, applications, and/or networks.
- Cloudflare processes web traffic information on behalf of its customers.

Customer data retention is defined by Cloudflare retention policies, when a customer is terminated, the data will be deleted per the retention policy. Customers may request for their data to be purged, in those instances, a data deletion script is run to purge customer data from production systems.

Customer data is encrypted at rest and in transit use AES 256-bit encryption, the management of keys are the responsibility of the cloud service providers.

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 following services provided by subservice organizations were not included within the scope of this examination:

- AWS and GCP – provides cloud hosting services for security, storage, data backup, and computing.

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

Control Activities Expected to be Implemented by Subservice Organizations	Applicable Trust Services Criteria
AWS and GCP are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where Cloudflare systems reside.	CC6.1 – CC6.3, CC6.5 – CC6.6
AWS and GCP are responsible for restricting physical access to facilities housing the Cloudflare systems to authorized personnel.	CC6.4 – CC6.5
AWS and GCP are responsible for implementing controls that ensure the data center facilities are equipped with physical and environmental security safeguards.	A1.2

CONTROL ENVIRONMENT

The control environment at Cloudflare 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 security leadership.

Integrity and Ethical Values

Senior management believes that strong ethical standards are essential elements to Cloudflare’s control environment. The effectiveness of controls cannot rise above the integrity and ethical values of the employees who create, administer, and monitor them. As such, integrity and ethical values are essential elements of Cloudflare’s control environment, affecting the design, administration, and monitoring of other components. The overarching business principle and code of conduct contained within the employee handbook help to define the core values of integrity for individuals that are part of the company’s culture and critical to managing the business. New hires are required to pass a background check and acknowledge and agree to Cloudflare’s policies and procedures, including the employee handbook, confidentiality agreement, and acceptable use policy, as a condition of their employment. Employees also complete the business code of conduct training upon hire.

Board of Directors and Security Leadership Oversight

Cloudflare’s control awareness is significantly influenced by its board of directors and security leadership team. The board of directors, which is composed of Cloudflare management and independent directors, meets quarterly to provide oversight, evaluate security risk and compliance initiatives, and provide guidance to meet ongoing business objectives. Cloudflare security leadership meets at least monthly to monitor and allocate resources to critical projects and to review information security related issues, inquiries, complaints, and disputes.

Organizational Structure and Assignment of Authority and Responsibility

The Cloudflare organizational structure provides the framework in which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Cloudflare’s organizational structure helps ensure that reporting lines, authorities and responsibilities are assigned to support security, availability, and confidentiality commitments. Roles and responsibilities for the governance of information security within Cloudflare are formally documented within the information security management standard and communicated via the Cloudflare intranet.

Commitment to Competence

Cloudflare defines competence as the knowledge and skills necessary to accomplish tasks within an employee's roles and responsibilities. Cloudflare's commitment to competence includes management's consideration of competence levels for positions and how those levels translate into skills and knowledge. Candidates' abilities to meet the requirements detailed in job descriptions are evaluated and documented during the hiring process and employees are required to pass a background check as a condition of their employment. Employees complete security awareness training upon hire, which includes information on threats, vulnerabilities, best practices, and how to report security events to the detection and response team. Cloudflare uses bi-weekly all-hands presentations to develop and retain personnel. Training courses are also available to employees via a company-wide learning management system.

Accountability

Management establishes accountability by setting a strong tone at the top and holding those accountable for internal control responsibilities. Management communicates the internal control responsibilities and the criteria that employees will be measured against as well as incentives and other rewards. Control owners review the design of internal controls annually and corrective actions related to identified deficiencies are tracked to resolution. Cloudflare has established a formal organizational structure to help ensure that reporting lines, authorities, and responsibilities are assigned to support Cloudflare's security, availability, and confidentiality commitments. Roles and responsibilities for the governance of information security within Cloudflare are formally documented within the information security management standard and communicated via the Cloudflare intranet.

RISK ASSESSMENT

Risk management is an iterative process where Cloudflare attempts to reduce business risk by undertaking an annual information security risk assessment to identify its critical assets, the threats facing those assets, and the likelihood and impact of the security of the assets that could be compromised. The established process addresses risks related to user and third-party management, applicable laws and regulations, and contractual requirements that may affect the system's security, confidentiality, and availability commitments.

Objective Setting

As part of the risk management program, Cloudflare management meets at least annually to discuss new and ongoing risks. The results of the meeting are documented in the risk assessment report and remediation is tracked in the risk register and continuously monitored by the security team. The annual risk assessment report is delivered to management, the chief security officer (CSO), and assigned risk owners. The security team works with management and stakeholders to determine appropriate risk treatment plans. Any risk mitigation plans are tracked in the risk register and risk acceptance is formally documented. The risk assessment and mitigation process serve to help ensure that existing controls adequately facilitate the achievement of Cloudflare's objectives for security, availability, and confidentiality of the company's and customers' data.

Risk Identification and Analysis

Cloudflare's security team performs an annual risk assessment to identify, assess, and plan for risks that could affect the organization's ability to provide reliable services to their users. The assessment includes analysis of potential errors, accidents, and acts of nature. The identification of risks can be informed by Cloudflare's objectives; operational observations; metrics from monitoring tools; internal and external assessments; analysis of significant changes to the organization or service; and evolving developments in the threat landscape.

Risk analysis is an essential process in Cloudflare's risk assessment process. An analysis of the likelihood and impact of the risk occurring is performed and a quantifiable risk score to the identified risk is assigned as a result.

Unacceptable risk scores trigger analysis of potential risk mitigation strategies documented within risk remediation plans and are assigned risk owners.

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 and pressures for employees
- Fraud opportunities
- 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

Cloudflare considers the pressures, opportunities, and motivation for fraud when assessing the risks to the achievement of Cloudflare's objectives. The potential for fraud can occur in both financial and non-financial reporting. Other types of fraud include the misappropriation of assets and illegal acts such as violations of governmental laws.

Management realizes that the potential for fraud can occur 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; therefore, Cloudflare's annual risk assessment considers the potential for fraud.

Risk Mitigation

Cloudflare performs an annual risk assessment and results from the risk assessment activities are reviewed by management to prioritize mitigation of identified risks. Cloudflare prepares a remediation plan to formally manage the resolution of findings identified in risk assessment 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, availability, and confidentiality categories.

Selection and Development of Control Activities

A suite of controls is maintained to help comply with external laws, regulations, industry requirements, and internal information security policies.

The applicable trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Cloudflare's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the Area 1 service.

INFORMATION AND COMMUNICATION SYSTEMS

Cloudflare identifies, captures, and communicates pertinent information in a form and timeframe that enables personnel to carry out their responsibilities. Information systems produce reports containing operational, financial, and compliance-related information that make it possible to run and control the business. Cloudflare 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 also occurs in a broader sense, flowing down, across and up the organization. Personnel receive a clear message from top management that control responsibilities must be taken seriously. Personnel must understand their own role in the internal control system, as well as how individual activities relate to the work of others.

Internal Communication

Cloudflare has implemented various methods of internally communicating information including objectives and responsibilities necessary to support the functioning of internal control. Cloudflare maintains information security policies and standards that are reviewed, approved by management, and communicated to personnel annually. New hires are required to acknowledge and agree to Cloudflare policies and procedures as a condition of their employment. Security management conducts monthly staff meetings to communicate and align on relevant security threats, program performance, policy review, and best practices. Roles and responsibilities for the governance of information security within Cloudflare are formally documented within the information security management standard and communicated on the Cloudflare intranet. Cloudflare has established an anonymous reporting hotline which is communicated to employees in the employee guidebook.

External Communication

Cloudflare has also implemented various methods of communicating with external parties regarding matters affecting the functioning of internal control. The customer support team has established policies and procedures for handling customer-reported incidents. Cloudflare provides a contact method for external parties to submit complaints and inquiries and report incidents. Cloudflare has also documented, and made available on their website, security-related documents that describe user accessibility, security features, and methods for user interaction.

When new enterprise customers sign-up to use Cloudflare's products, the enterprise customer is required to sign a master subscription agreement which includes considerations for protecting the security, availability, and confidentiality of the data and indicates the responsibilities of the users and Cloudflare's responsibilities and commitments. When new free, business, and professional plan customers sign-up to use Cloudflare's products, the customer digitally consents to the self-serve subscription agreement which includes considerations for protecting the security, availability, and confidentiality of the data and indicates the responsibilities of the customers.

MONITORING

Cloudflare's monitoring process assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing monitoring activities, separate evaluations, and monitoring of Cloudflare's subservice organizations.

Ongoing Monitoring and Separate Evaluations

Control owners review the design of internal controls annually. Corrective actions related to identified deficiencies are tracked to resolution. Cloudflare also has annual internal and external audits performed on information systems and processes. An internal audit program is in place which includes guidance on the frequency, methods, and responsibilities of the audit; consideration of the results of previous audits; audit criteria and scope; and the reporting of results to management. Internal audits are performed annually and the audit results, including corrective action plans for identified control deficiencies, are documented and reviewed by management and tracked to resolution.

Vendor and Subservice Organization Monitoring

Third-party vendors play an important role in the support of Cloudflare processes. Setting appropriate limits and controls on third-party vendors helps reduce the risk of security incidents, financial liability, and reputational risk. Therefore, Cloudflare reviews the security impact of third-party service providers in accordance with a defined third-party risk management process prior to engagement. For service providers classified as critical, high, and moderate impact, Cloudflare annually reviews third-party attestation reports, security questionnaires, or service provider reported information security controls. If control gaps are identified, action is taken to address the impact on the organization.

Agreements containing information security requirements and confidentiality obligations are also in place with moderate, high, and critical impact third-party service providers.

Evaluating and Communicating Deficiencies

The board of directors, which is composed of Cloudflare management and independent directors, meets quarterly to provide oversight, evaluate security risk and compliance initiatives, and provide guidance to meet ongoing business objectives.

Security management conducts monthly staff meetings to communicate and align on relevant security threats, program performance, policy review, and best practices. Cloudflare security leadership meets at least monthly to monitor and allocate resources to critical projects and review information security related issues, inquiries, complaints, and disputes.

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 Area 1 service provided by Cloudflare. The scope of the testing was restricted to the Area 1 service and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period January 1, 2023, to March 31, 2023.

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. 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	New hires are required to acknowledge and agree to Cloudflare policies and procedures as a condition of their employment.	Inspected the policy acknowledgement for a sample of employees hired during the period to determine that each sampled employee acknowledged and agreed to Cloudflare policies and procedures as a condition of their employment.	No exceptions noted.
CC1.1.2	New hire employees are required to complete the business code of conduct acknowledgement upon hire.	Inspected the code of conduct acknowledgement record for a sample of new hire employees to determine that new hire employees completed the business code of conduct acknowledgement upon hire.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.3	New hire employees are required to pass a background check as a condition of their employment. Exceptions must be approved by the security and legal teams.	Inquired with the security compliance manager to determine that new hire employees were passed a background check and exceptions as a result of the background check approved by the security and legal teams.	No exceptions noted.
		Inspected background checks for a sample of employees hired during the period to determine that each sampled new hire employee passed a background check as a condition of their employment.	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, which is composed of Cloudflare management and independent directors, meets quarterly to provide oversight, evaluate security risk and compliance initiatives, and provide guidance to meet ongoing business objectives.	Inspected the board of directors member listing on Cloudflare's public governance website to determine that the board of directors included independent directors.	No exceptions noted.
		Inspected the board meeting minutes for a sample of quarters during the period to determine that the board of directors met during each sampled quarter to provide oversight, evaluate security risk and compliance initiatives, and provide guidance to meet ongoing business objectives.	No exceptions noted.
CC1.2.2	Cloudflare security leadership meets at least monthly to: <ul style="list-style-type: none">Monitor and allocate resources to projectsReview information security related issues, inquiries, complaints, and disputes	Inspected the security leadership meeting invite and minutes for a sample of months during the period to determine that Cloudflare security leadership met during each sampled month to: <ul style="list-style-type: none">Monitor and allocate resources to projectsReview information security related issues, inquiries, complaints, and disputes	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	Cloudflare has established a formal organizational structure to help ensure that reporting lines, authorities, and responsibilities are assigned to support Cloudflare's security, availability, and confidentiality commitments.	Inspected Cloudflare's organizational chart to determine that Cloudflare had established a formal organizational structure to ensure that reporting lines, authorities, and responsibilities were assigned to support Cloudflare's security, availability, and confidentiality commitments.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3.2	Roles and responsibilities for the governance of information security within Cloudflare are formally documented within the information security management standard and communicated via the Cloudflare intranet.	Inspected the information security management standard on Cloudflare's intranet to determine that roles and responsibilities for the governance of information security within Cloudflare were formally documented within the information security management standard and communicated via the Cloudflare intranet.	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 hire employees are required to pass a background check as a condition of their employment. Exceptions must be approved by the security and legal teams.	Inquired with the security compliance manager to determine that new hire employees passed a background check and exceptions as a result of the background check were approved by the security and legal teams.	No exceptions noted.
		Inspected background checks for a sample of employees hired during the period to determine that each sampled new hire employee passed a background check as a condition of their employment.	No exceptions noted.
CC1.4.2	Candidates' abilities to meet the requirements detailed in job descriptions are evaluated and documented during the hiring process.	Inspected the candidate evaluation for a sample of employees hired during the period to determine that candidates' abilities to meet the requirements detailed in job descriptions were evaluated during the hiring process for each sampled employee.	No exceptions noted.
CC1.4.3	Employees complete security awareness training upon hire which includes information on threats, vulnerabilities, best practices, and how to report security events to the detection and response team.	Inspected the security awareness training records for a sample of employees hired during the period to determine that each sampled employee completed security awareness training upon hire which included information on threats, vulnerabilities, best practices, and how to report security events to the detection and response team.	No exceptions noted.
CC1.4.4	Cloudflare uses bi-weekly all-hands presentations to develop and retain personnel.	Inspected the recurring all-hands meeting calendar invite and an example meeting agenda for a meeting held during the period to determine that Cloudflare used bi-weekly all-hands presentations to develop and retain personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.5	Training courses are made available to employees via a company-wide learning management system.	Inspected the learning management system dashboard to determine that training courses were made available to employees via the company-wide learning management system.	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	Cloudflare has established a formal organizational structure to help ensure that reporting lines, authorities, and responsibilities are assigned to support Cloudflare's security, availability, and confidentiality commitments.	Inspected Cloudflare's organizational chart to determine that Cloudflare had established a formal organizational structure to ensure that reporting lines, authorities, and responsibilities were assigned to support Cloudflare's security, availability, and confidentiality commitments.	No exceptions noted.
CC1.5.2	Control owners review the design of internal controls annually. Corrective actions related to identified deficiencies are tracked to resolution.	Inspected the most recent control attestation ticket to determine that control owners reviewed the design of internal controls during the period and that corrective actions related to identified deficiencies were tracked to resolution.	No exceptions noted.
CC1.5.3	Roles and responsibilities for the governance of information security within Cloudflare are formally documented within the information security management standard and communicated on the company intranet.	Inspected the information security management standard and Cloudflare's internal Wiki to determine that roles and responsibilities for the governance of information security within Cloudflare were formally documented within the information security management standard and communicated on the company intranet.	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	Control owners review the design of internal controls annually. Corrective actions related to identified deficiencies are tracked to resolution.	Inspected the most recent control attestation ticket to determine that control owners reviewed the design of internal controls during the period and that corrective actions related to identified deficiencies were tracked to resolution.	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	New hires are required to acknowledge and agree to Cloudflare policies and procedures as a condition of their employment.	Inspected the policy acknowledgement for a sample of employees hired during the period to determine that each sampled employee acknowledged and agreed to Cloudflare policies and procedures as a condition of their employment.	No exceptions noted.
CC2.2.2	Cloudflare has established an anonymous reporting hotline which is communicated to employees in the employee guidebook.	Inspected the employee guidebook and anonymous reporting hotline website to determine that Cloudflare has established an anonymous reporting hotline and communicated the process to employees in the employee guidebook.	No exceptions noted.
CC2.2.3	Cloudflare maintains information security policies and standards that are reviewed, approved by management, and communicated to personnel annually.	Inspected the information security policies and standards on the Cloudflare intranet to determine that Cloudflare maintained information security policies and standards that were reviewed, approved by management, and communicated to authorized personnel during the period.	No exceptions noted.
CC2.2.4	Security management conducts monthly staff meeting to communicate and align on relevant security threats, program performance, policy review, and best practices.	Inspected the security management recurring meeting invite and meeting agenda for a sample of months during the period to determine that security management conducted a staff meeting for each sampled month to communicate and align on relevant security threats, program performance, policy review, and best practices.	No exceptions noted.
CC2.2.5	Roles and responsibilities for the governance of information security within Cloudflare are formally documented within the information security management standard and communicated on the company intranet.	Inspected the information security management standard and Cloudflare's internal Wiki to determine that roles and responsibilities for the governance of information security within Cloudflare were formally documented within the information security management standard and communicated on the company intranet.	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	The customer support team has established policies and procedures for handling customer-reported incidents. Cloudflare provides a contact method for external parties to submit complaints and inquiries and report incidents.	Inspected Cloudflare's customer incident management policy to determine that the customer support team has established policies and procedures for handling customer-reported incidents.	No exceptions noted.
		Inspected Cloudflare's website support page to determine that Cloudflare provided a contact method for external parties to submit complaints and inquiries and report incidents.	No exceptions noted.
CC2.3.2	Cloudflare has documented, and made available on their website, security-related documents that describe user accessibility, security features, and methods for user interaction.	Inspected the Cloudflare support webpage and the Cloudflare system status webpage to determine that Cloudflare had documented, and made available on their website, security-related documents that described user accessibility, security features, and methods for user interaction.	No exceptions noted.
CC2.3.3	Customers are required to sign a master subscription agreement during onboarding which includes considerations for protecting the security, availability, and confidentiality of the data and indicates the responsibilities of the users and Cloudflare's responsibilities and commitments.	Inspected the master subscription agreement for a sample of new customers during the period to determine that each sampled customer signed the master subscription agreement during the period which included considerations for protecting the security, availability, and confidentiality of data and indicated the responsibilities of the users and Cloudflare's responsibilities and commitments.	No exceptions noted.
CC2.3.4	Customers are required to digitally consent to the self-serve subscription agreement during onboarding which includes considerations for protecting the security, availability, and confidentiality of the data and indicates the responsibilities of the customers.	Inspected the customer sign-up page and self-serve subscription agreement to determine that customers digitally consented to Cloudflare's self-serve subscription agreement which included considerations for protecting the security, availability, and confidentiality of the data and indicated the responsibilities of the customers.	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	Cloudflare identifies the business impact of relevant threats to assets, infrastructure, and resources that support core business functions.	Inspected the most recent risk assessment performed during the period to determine that Cloudflare identified the business impact of relevant threats to assets, infrastructure, and resources that support core business functions.	No exceptions noted.
CC3.1.2	Security management conducts monthly staff meeting to communicate and align on relevant security threats, program performance, policy review, and best practices.	Inspected the security management recurring meeting invite and meeting agenda for a sample of months during the period to determine that security management conducted a staff meeting for each sampled month to communicate and align on relevant security threats, program performance, policy review, and best practices.	No exceptions noted.
CC3.1.3	The board of directors, which is composed of Cloudflare management and independent directors, meets quarterly to provide oversight, evaluate security risk and compliance initiatives, and provide guidance to meet ongoing business objectives.	Inspected the board of directors member listing on Cloudflare's public governance website to determine that the board of directors included independent directors.	No exceptions noted.
		Inspected the board meeting minutes for a sample of quarters during the period to determine that the board of directors met during each sampled quarter to provide oversight, evaluate security risk and compliance initiatives, and provide guidance to meet ongoing business objectives.	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	Cloudflare performs a risk assessment annually. Results from risk assessment activities are reviewed by management to prioritize mitigation of identified risks.	Inspected the most recent risk assessment and security leadership risk assessment meeting agenda performed during the period to determine that Cloudflare performed a risk assessment during the period and that results from risk assessment activities were reviewed by management and prioritized to mitigate identified risks.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.2	Cloudflare has internal and external audits performed on information systems and processes annually. Findings identified from the audits are tracked to resolution.	Inspected the internal audit program, audit calendar, and internal audit executive summary report to determine that Cloudflare had internal and external audits performed on information systems and processes during the period.	No exceptions noted.
		Inspected the most recent internal audit performed to determine that findings identified from the audits were tracked to resolution.	No exceptions noted.
CC3.2.3	Cloudflare prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the most recent risk assessment, risk register, and risk treatment procedures to determine that Cloudflare prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	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	Cloudflare performs a risk assessment annually that considers the potential for fraud. Results from risk assessment activities are reviewed by management to prioritize mitigation of identified risks.	Inspected the most recent risk assessment and security leadership risk assessment meeting agenda performed during the period to determine that Cloudflare performed a risk assessment during the period that considered the potential for fraud and that results from risk assessment activities were reviewed by management and prioritized to mitigate identified risks.	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	Cloudflare performs a risk assessment annually. Results from risk assessment activities are reviewed by management to prioritize mitigation of identified risks.	Inspected the most recent risk assessment and security leadership risk assessment meeting agenda performed during the period to determine that Cloudflare performed a risk assessment during the period and that results from risk assessment activities were reviewed by management and prioritized to mitigate identified risks.	No exceptions noted.
CC3.4.2	Control owners review the design of internal controls annually. Corrective actions related to identified deficiencies are tracked to resolution.	Inspected the most recent control attestation ticket to determine that control owners reviewed the design of internal controls during the period and that corrective actions related to identified deficiencies were tracked to resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4.3	Cloudflare has internal and external audits performed on information systems and processes annually. Findings identified from the audits are tracked to resolution.	Inspected the internal audit program, audit calendar, and internal audit executive summary report to determine that Cloudflare had internal and external audits performed on information systems and processes during the period.	No exceptions noted.
		Inspected the most recent internal audit performed to determine that findings identified from the audits were tracked to resolution.	No exceptions noted.
CC3.4.4	Cloudflare prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the most recent risk assessment, risk register, and risk treatment procedures to determine that Cloudflare prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	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	Control owners review the design of internal controls annually. Corrective actions related to identified deficiencies are tracked to resolution.	Inspected the most recent control attestation ticket to determine that control owners reviewed the design of internal controls during the period and that corrective actions related to identified deficiencies were tracked to resolution.	No exceptions noted.
CC4.1.2	Cloudflare has internal and external audits performed on information systems and processes annually. Findings identified from the audits are tracked to resolution.	Inspected the internal audit program, audit calendar, and internal audit executive summary report to determine that Cloudflare had internal and external audits performed on information systems and processes during the period.	No exceptions noted.
		Inspected the most recent internal audit performed to determine that findings identified from the audits were tracked to resolution.	No exceptions noted.
CC4.1.3	Cloudflare performs an annual review of third-party attestation reports, security questionnaires, or service provider reported information security controls for high impact service providers. If control gaps are identified, action is taken to address impact on the organization.	Inspected the management review documentation for a sample of impact service providers classified as high impact by Cloudflare to determine that Cloudflare reviewed third-party attestation reports, security questionnaires, or service provider reported information security controls for high impact service providers during the period and that action was taken on control gaps to address impact on the organization, if applicable.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.4	Prior to engagement, Cloudflare reviews the security impact of third-party service providers in accordance with a defined third-party risk management process. For moderate and high impact service providers, Cloudflare reviews third-party attestation reports, security questionnaires, or service provider reported information security controls. If control gaps are identified, action is taken to address impact on the organization.	Inspected the vendor security review documentation for a sample of third-party service providers contracted during the period that were classified by Cloudflare as moderate and high to determine that Cloudflare reviewed the security impact of third-party service providers including third-party attestation reports, security questionnaires, or service provider reported information security controls during the period for each sampled service provider and that action was taken for identified control gaps to address the impact on the organization, if applicable.	No exceptions noted.
CC4.1.5	Cloudflare utilizes a tool to scan source code for vulnerabilities.	Inspected the source code vulnerability scanning tool configuration to determine that Cloudflare utilized a tool to scan source code for vulnerabilities.	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	Security management conducts monthly staff meeting to communicate and align on relevant security threats, program performance, policy review, and best practices.	Inspected the security management recurring meeting invite and meeting agenda for a sample of months during the period to determine that security management conducted a staff meeting for each sampled month to communicate and align on relevant security threats, program performance, policy review, and best practices.	No exceptions noted.
CC4.2.2	The board of directors, which is composed of Cloudflare management and independent directors, meets quarterly to provide oversight, evaluate security risk and compliance initiatives, and provide guidance to meet ongoing business objectives.	Inspected the board of directors member listing on Cloudflare's public governance website to determine that the board of directors included independent directors.	No exceptions noted.
		Inspected the board meeting minutes for a sample of quarters during the period to determine that the board of directors met during each sampled quarter to provide oversight, evaluate security risk and compliance initiatives, and provide guidance to meet ongoing business objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.3	Cloudflare security leadership meets at least monthly to: <ul style="list-style-type: none"> • Monitor and allocate resources to projects • Review information security related issues, inquiries, complaints, and disputes 	Inspected the security leadership meeting invite and minutes for a sample of months during the period to determine that Cloudflare security leadership met during each sampled month to: <ul style="list-style-type: none"> • Monitor and allocate resources to projects • Review information security related issues, inquiries, complaints, and disputes 	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	Cloudflare performs a risk assessment annually. Results from risk assessment activities are reviewed by management to prioritize mitigation of identified risks.	Inspected the most recent risk assessment and security leadership risk assessment meeting agenda performed during the period to determine that Cloudflare performed a risk assessment during the period and that results from risk assessment activities were reviewed by management and prioritized to mitigate identified risks.	No exceptions noted.
CC5.1.2	Cloudflare prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the most recent risk assessment, risk register, and risk treatment procedures to determine that Cloudflare prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.
CC5.1.3	A suite of controls is maintained to help comply with external laws, regulations, industry requirements, and internal information security policies.	Inspected Cloudflare's control listing to determine that a suite of controls was maintained to help comply with external laws, regulations, industry requirements, and internal information security policies.	No exceptions noted.
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	Cloudflare performs a risk assessment annually. Results from risk assessment activities are reviewed by management to prioritize mitigation of identified risks.	Inspected the most recent risk assessment and security leadership risk assessment meeting agenda performed during the period to determine that Cloudflare performed a risk assessment during the period and that results from risk assessment activities were reviewed by management and prioritized to mitigate identified risks.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2.2	Cloudflare prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the most recent risk assessment, risk register, and risk treatment procedures to determine that Cloudflare prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.
CC5.2.3	A suite of controls is maintained to help comply with external laws, regulations, industry requirements, and internal information security policies.	Inspected Cloudflare's control listing to determine that Cloudflare maintained a suite of controls to help comply with external laws, regulations, industry requirements, and internal information security policies.	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	New hires are required to acknowledge and agree to Cloudflare policies and procedures as a condition of their employment.	Inspected the policy acknowledgement for a sample of employees hired during the period to determine that each sampled employee acknowledged and agreed to Cloudflare policies and procedures as a condition of their employment.	No exceptions noted.
CC5.3.2	Cloudflare maintains information security policies and standards that are reviewed, approved by management, and communicated to personnel annually.	Inspected the information security policies and standards on the Cloudflare intranet to determine that Cloudflare maintained information security policies and standards that were reviewed, approved by management, and communicated to authorized personnel during the period.	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	Sensitive data transmitted over public networks is encrypted.	Inspected Cloudflare's encryption certificate on the customer dashboard to determine that sensitive data transmitted over public networks was encrypted.	No exceptions noted.
CC6.1.2	Customer keys are encrypted and stored on encrypted drives.	Inspected the customer key encryption configuration and the drive in which the keys were stored to determine that customer keys were encrypted and stored on encrypted drives.	No exceptions noted.
CC6.1.3	Access to the cryptographic keystores is limited to authorized personnel.	Inspected a system generated list of individuals with access to the cryptographic keystores and their associated job titles to determine that access to cryptographic keystores was limited to authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.4	Cloudflare requires unique identifiers for user accounts and prevents identifier reuse.	Inspected a system generated list of user accounts to determine that Cloudflare required unique identifiers for user accounts and prevented identifier reuse.	No exceptions noted.
CC6.1.5	User and device authentication to information systems is protected by passwords that meet Cloudflare's password complexity and multi-factor requirements.	Inspected the SSO configurations to determine that user and device authentication to information systems was protected by passwords that met Cloudflare's password complexity and multi-factor requirements.	No exceptions noted.
CC6.1.6	Multi-factor authentication is required for remote sessions and access to the production environment.	Inspected the Okta multi-factor configuration screenshots to determine that multi-factor authentication was required for remote sessions and access to the production environment.	No exceptions noted.
CC6.1.7	Access to modify endpoint utility programs is limited to authorized individuals.	Inspected a system generated listing of users with access to modify endpoint utility programs and their associated job titles with the assistance of the security compliance specialist to determine that access was limited to authorized personnel.	No exceptions noted.
CC6.1.8	Break glass actions are logged, and access must be allowed by account admins. Employees with access to make changes to customer accounts are restricted only to authorized personnel.	Inspected the editing permissions, logging configurations, and an example log during the period to determine that break glass actions are logged, and access must be allowed by account admins.	No exceptions noted.
		Inspected a system generated list of user accounts with access to make changes to customer accounts with the assistance of the security compliance specialist to determine that access to make changes to customer accounts was restricted to authorized personnel.	No exceptions noted.
AWS and GCP are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where Cloudflare 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	Logical access provisioning to information systems is based on default job groups. Additional approval is required for access provisioned outside of the default job groups.	Inspected the access provisioning ticket for a sample of access requests processed during the period to determine that logical access to information systems was provisioned based on the default job group and additional approval was obtained for access provisioned outside of the default job groups of each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.2	Logical access that is no longer required in the event of a termination is documented, communicated to IT, and revoked.	Inspected the termination ticket and in-scope system user account listings for a sample of employees terminated during the period to determine that logical access that was no longer required in the event of a termination was documented, communicated to IT, and revoked.	No exceptions noted.
CC6.2.3	Cloudflare performs account and access reviews quarterly and corrective action is taken, when applicable.	Inspected the access review tickets for a sample of quarters during the period to determine that Cloudflare performed account and access reviews for each sampled quarter and that corrective action were taken where applicable.	No exceptions noted.
CC6.2.4	Upon an employee's reassignment or transfer, access that is no longer required is revoked and documented.	Inspected the transfer ticket for a sample of employee reassigned or transferred during the period to determine that access that was no longer required was revoked and documented.	No exceptions noted.
AWS and GCP are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where Cloudflare 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	Logical access provisioning to information systems is based on default job groups. Additional approval is required for access provisioned outside of the default job groups.	Inspected the access provisioning ticket for a sample of employees hired during the period to determine that logical access to information systems was provisioned based on the default job group and additional approval was obtained for access provisioned outside of the default job groups or each employee sampled.	No exceptions noted.
CC6.3.2	Logical access that is no longer required in the event of a termination is documented, communicated to IT, and revoked.	Inspected the termination ticket and in-scope system user account listings for a sample of employees terminated during the period to determine that logical access that was no longer required in the event of a termination was documented, communicated to IT, and revoked.	No exceptions noted.
CC6.3.3	Cloudflare performs account and access reviews quarterly and corrective action is taken, when applicable.	Inspected the access review tickets for a sample of quarters during the period to determine that Cloudflare performed account and access reviews for each sampled quarter and that corrective action were taken where applicable.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.4	Upon an employee's reassignment or transfer, access that is no longer required is revoked and documented.	Inspected the transfer ticket for a sample of employee reassigned or transferred during the period to determine that access that was no longer required was revoked and documented.	No exceptions noted.
	AWS and GCP are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where Cloudflare 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.			
	AWS and GCP are responsible for restricting physical access to facilities housing the Cloudflare systems 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.			
	AWS and GCP are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where Cloudflare systems reside.		
	AWS and GCP are responsible for restricting physical access to facilities housing the Cloudflare systems 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	Multi-factor authentication is required for remote sessions and access to the production environment.	Inspected the Okta multi-factor configuration screenshots to determine that multi-factor authentication was required for remote sessions and access to the production environment.	No exceptions noted.
CC6.6.2	Network traffic to and from untrusted networks passes through a policy enforcement point.	Inspected the firewall rulesets to determine that network traffic to and from untrusted networks passed through a policy enforcement point.	No exceptions noted.
CC6.6.3	Cloudflare utilizes a web application firewall in front of public-facing web applications to detect and prevent web-based attacks.	Inspected the web application firewall configuration to determine that Cloudflare utilized a web application firewall in front of public-facing web applications to detect and prevent web-based attacks.	No exceptions noted.
	AWS and GCP are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where Cloudflare 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	Cloudflare maintains policies and procedures for the secure handling of media including: <ul style="list-style-type: none">Secure erasure of mediaSecure handling of mediaManagement of removable media	Inspected the media protection policy and the hardware recycling process document to determine that Cloudflare maintained policies and procedures for the secure handling of media including: <ul style="list-style-type: none">Secure erasure of mediaSecure handling of mediaManagement of removable media	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.7.2	Sensitive data transmitted over public networks is encrypted.	Inspected Cloudflare's encryption certificate on dashboard to determine that sensitive data transmitted over public networks was encrypted.	No exceptions noted.
CC6.7.3	The databases are configured to encrypt customer data at rest.	Inspected the data at rest encryption configurations to determine that the databases were configured to encrypt customer data at rest.	No exceptions noted.
CC6.7.4	Employee workstations are protected with full disk encryption.	Inspected the encryption configurations for a sample of employee workstations to determine that each sampled employee workstation was protected with full disk encryption.	No exceptions noted.
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	Hardening and baseline configuration standards have been established according to industry standards and are reviewed and updated at least annually.	Inspected the security hardening and baseline configuration standards and the most recent review to determine that security hardening and baseline configuration standards were established and were reviewed and updated during the period.	No exceptions noted.
CC6.8.2	Cloudflare uses mechanisms to detect deviations from baseline configurations in production environments.	Inspected the alerting configurations and a selected alert for a baseline deviation to determine that Cloudflare uses monitoring tools to detect deviations from baseline configurations in production environments.	No exceptions noted.
CC6.8.3	Access to modify endpoint utility programs is limited to authorized individuals.	Inspected a system generated listing of users with access to modify endpoint utility programs and their associated job titles with the assistance of the security compliance specialist to determine that access was limited to authorized personnel.	No exceptions noted.
CC6.8.4	A device management tool is configured to check employee workstations for security-relevant patches at least daily and install software and/or firmware updates, as applicable.	Inspected the device management tool configurations and patching history during the period for a sample of employee workstations to determine that a device management tool was configured to check each sampled employee workstation for a security-relevant patches at least daily and install software and/or firmware updates, as applicable.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.8.5	Enterprise antivirus software is installed to protect employee workstations. The ability to disable antivirus on workstations is restricted.	Inspected the antivirus configurations for a sample of employee workstations to determine that enterprise antivirus software was installed on each employee workstation sampled.	No exceptions noted.
		Inspected the device management tool anti-tampering configuration and administrator user account listing to determine that the ability to disable antivirus on workstations was restricted.	No exceptions noted.
CC6.8.6	Security patches are released automatically to in-scope servers through a configuration system to help ensure current patches are implemented.	Inspected the security patching configuration and example log during the period to determine that security patches were released automatically to servers to help ensure current patches were implemented.	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	Hardening and baseline configuration standards have been established according to industry standards and are reviewed and updated at least annually.	Inspected the security hardening and baseline configuration standards and the most recent review to determine that security hardening and baseline configuration standards were established and were reviewed and updated during the period.	No exceptions noted.
CC7.1.2	Cloudflare uses mechanisms to detect deviations from baseline configurations in production environments.	Inspected the monitoring configurations and an example alert generated during the period to determine that Cloudflare used mechanisms to detect deviations from baseline configurations in production environments.	No exceptions noted.
CC7.1.3	Cloudflare conducts internal vulnerability scans at least quarterly to identify potential high vulnerabilities which are researched and resolved.	Inspected the vulnerability scan report and remediation tickets for a sample of quarters during the period to determine that Cloudflare conducted internal vulnerability scans for each sampled quarter to identify potential high vulnerabilities which were researched and resolved.	No exceptions noted.
CC7.1.4	Cloudflare conducts penetration tests at least annually. Issues that exceed a predefined threshold are tracked through resolution.	Inspected the most recent penetration test results and remediation tickets to determine that Cloudflare conducted penetration tests during the period and that issues that exceed a predefined threshold were identified and tracked through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	Cloudflare logs information system activity to a secure repository. The number of administrators with access to audit logs is limited.	Inspected the storage log and system generated list of users with administration access to the audit logs to determine that Cloudflare logged information system activity to a secure repository and that the number of administrators with access to audit logs was limited.	No exceptions noted.
CC7.2.2	Production systems are monitored in accordance with predefined security criteria and alerts are sent to authorized personnel. Confirmed incidents are tracked to resolution.	Inspected the security monitoring tool configurations and example incident ticket to determine that production systems were monitored in accordance with predefined security criteria, alerts were sent to authorized personnel, and confirmed incidents were tracked to resolution.	No exceptions noted.
CC7.2.3	Cloudflare defines availability monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	Inspected the availability monitoring configurations and example ticket for an availability alert generated during the period to determine that Cloudflare defined availability monitoring alert criteria, how alert criteria was flagged, and identified authorized personnel for flagged system alerts.	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	Cloudflare maintains an incident response plan that defines the type of incidents that need to be managed, tracked, and reported.	Inspected the incident response plan to determine that Cloudflare maintained an incident response plan that defines the type of incidents that need to be managed, tracked, and reported.	No exceptions noted.
CC7.3.2	Confirmed incidents are assigned a priority level and managed to resolution. The incident response team performs a postmortem for incidents classified as P0 or P1.	Inspected the incident ticket for a sample of incidents identified during the period to determine that confirmed incidents were assigned a priority level and managed to resolution.	No exceptions noted.
		Inspected the incident ticket for a sample of incidents identified and classified as P0 or P1 during the period to determine that the incident response team performed a postmortem for incidents classified as P0 or P1.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3.3	Cloudflare logs information system activity to a secure repository. The number of administrators with access to audit logs is limited.	Inspected the storage log and system generated list of users with administration access to the audit logs to determine that Cloudflare logged information system activity to a secure repository and that the number of administrators with access to audit logs was limited.	No exceptions noted.
CC7.3.4	Production systems are monitored in accordance with predefined security criteria and alerts are sent to authorized personnel. Confirmed incidents are tracked to resolution.	Inspected the security monitoring tool configurations and example incident ticket to determine that production systems were monitored in accordance with predefined security criteria, alerts were sent to authorized personnel, and confirmed incidents were tracked to resolution.	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	Cloudflare maintains an incident response plan that defines the type of incidents that need to be managed, tracked, and reported.	Inspected the incident response plan to determine that Cloudflare maintained an incident response plan that defines the type of incidents that need to be managed, tracked, and reported.	No exceptions noted.
CC7.4.2	Confirmed incidents are assigned a priority level and managed to resolution. The incident response team performs a postmortem for incidents classified as P0 or P1.	Inspected the incident ticket for a sample of incidents identified during the period to determine that confirmed incidents were assigned a priority level and managed to resolution.	No exceptions noted.
		Inspected the incident ticket for a sample of incidents identified and classified as P0 or P1 during the period to determine that the incident response team performed a postmortem for incidents classified as P0 or P1.	No exceptions noted.
CC7.4.3	Cloudflare defines external communication requirements for incidents, including: <ul style="list-style-type: none"> Information about external party dependencies Criteria for notification to external parties as required by Cloudflare policy in the event of a security breach 	Inspected the security incident response policy to determine that Cloudflare defined external communication requirements for incidents, including: <ul style="list-style-type: none"> Information about external party dependencies Criteria for notification to external parties as required by Cloudflare policy in the event of a security breach 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Cloudflare's business continuity and disaster recovery plan is reviewed, approved by management, and communicated to relevant team members annually.	Inspected the business continuity and disaster recovery plan to determine that the plan was reviewed, approved by management, and communicated to relevant team members during the period.	No exceptions noted.
CC7.5.2	Cloudflare maintains emergency management documentation which is communicated to employees.	Inspected the Cloudflare emergency management page and an e-mail communication related to emergency procedures sent during the period to determine that Cloudflare maintains emergency management documentation which was communicated to employees during the period.	No exceptions noted.
CC7.5.3	Cloudflare configures redundant systems and performs daily backups of databases containing customer and end user data to resume system operations in the event of a system failure.	Inspected the database backup and replication configuration and a selected backup log for a database containing end-user or customer data and automated failed backup alert to determine that Cloudflare configured redundant systems and performs daily backups of databases containing customer and end user data to resume system operations in the event of a system failure.	No exceptions noted.
CC7.5.4	Cloudflare performs backup restoration and failover tests annually to confirm the reliability and integrity of system backups and recovery operations.	Inspected the most recent backup restoration and failover test results to determine that Cloudflare performed backup restoration and failover tests during the period.	No exceptions noted.
CC7.5.5	Cloudflare maintains an incident response plan that defines the types of incidents that need to be managed, tracked, and reported.	Inspected the security and privacy incident response policy to determine that Cloudflare maintained an incident response plan that defines the types of incidents that need to be managed, tracked, and reported.	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	Change management policies and procedures are documented to guide employees in making changes to production systems.	Inspected the SDLC and change management policy to determine that change management policies and procedures were documented to guide employees in making changes to production systems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.2	<p>Prior to introducing changes into the production environment, review and approval from authorized personnel is required based on the following:</p> <ul style="list-style-type: none"> • Change description • Impact of change • Test results 	<p>Inspected change ticket for a sample of changes implemented during the period to determine that each sampled change was reviewed and approved by authorized personnel prior implementation based on the following:</p> <ul style="list-style-type: none"> • Change description • Impact of change • Test results 	No exceptions noted.
CC8.1.3	The version control software is configured to require independent code review and approval by an individual other than the one who initiated the pull request.	Inspected the versions control software branch protection configurations and an example change ticket to determine that the version control software was configured to require independent code review and approval by an individual other than the one who initiated the pull request.	No exceptions noted.
CC8.1.4	Administrative access to the version control software is restricted to authorized personnel.	Inspected a system generated listing of users with access to the version control software to determine that administrative access to the version control software is restricted to authorized personnel.	No exceptions noted.
CC8.1.5	Branch protections are enabled to prevent a user from circumventing the approval requirements enforced by the version control software.	Inspected the version control script configuration to determine that branch protections were enabled to prevent a user from circumventing the approval requirements enforced by the version control software.	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	Cloudflare's business continuity and disaster recovery plan is reviewed, approved by management, and communicated to relevant team members annually.	Inspected the business continuity and disaster recovery plan to determine that the plan was reviewed, approved by management, and communicated to relevant team members during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.2	<p>Cloudflare performs a test of the business continuity and disaster recovery plan annually and ensures the following:</p> <ul style="list-style-type: none"> • Tests are executed with relevant contingency teams • Test results are documented • Corrective actions are taken for exceptions noted • Plans are updated based on results 	<p>Inspected the most recent business contingency and disaster recovery plan test to determine that Cloudflare performed a test of the business continuity and disaster recovery plan during the period and ensured the following:</p> <ul style="list-style-type: none"> • Tests were executed with relevant contingency teams • Test results were documented • Corrective actions were taken for exceptions noted • Plans were updated based on results 	No exceptions noted.
CC9.1.3	Cloudflare identifies the business impact of relevant threats to assets, infrastructure, and resources that support core business functions.	Inspected the most recent risk assessment performed during the period to determine that Cloudflare identified the business impact of relevant threats to assets, infrastructure, and resources that support core business functions.	No exceptions noted.
CC9.1.4	Cloudflare configures redundant systems and performs daily backups of databases containing customer and end user data to resume system operations in the event of a system failure.	Inspected the database backup and replication configuration and a selected backup log for a database containing end-user or customer data and automated failed backup alert to determine that Cloudflare configured redundant systems and performs daily backups of databases containing customer and end user data to resume system operations in the event of a system failure.	No exceptions noted.
CC9.1.5	Cloudflare performs backup restoration and failover tests annually to confirm the reliability and integrity of system backups and recovery operations.	Inspected the most recent backup restoration and failover test results to determine that Cloudflare performed backup restoration and failover tests during the period.	No exceptions noted.
CC9.1.6	Cloudflare performs a risk assessment annually. Results from risk assessment activities are reviewed by management to prioritize mitigation of identified risks.	Inspected the most recent risk assessment and security leadership risk assessment meeting agenda performed during the period to determine that Cloudflare performed a risk assessment during the period and that results from risk assessment activities were reviewed by management and prioritized to mitigate identified risks.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.7	Cloudflare prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the most recent risk assessment, risk register, and risk treatment procedures to determine that Cloudflare prepared a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Cloudflare performs an annual review of third-party attestation reports, security questionnaires, or service provider reported information security controls for high impact service providers. If control gaps are identified, action is taken to address impact on the organization.	Inspected the management review documentation for a sample of impact service providers classified as high impact by Cloudflare to determine that Cloudflare reviewed third-party attestation reports, security questionnaires, or service provider reported information security controls for high impact service providers during the period and that action was taken on control gaps to address impact on the organization, if applicable.	No exceptions noted.
CC9.2.2	Prior to engagement, Cloudflare reviews the security impact of third-party service providers in accordance with a defined third-party risk management process. For moderate and high impact service providers, Cloudflare reviews third-party attestation reports, security questionnaires, or service provider reported information security controls. If control gaps are identified, action is taken to address impact on the organization.	Inspected the vendor security review documentation for a sample of third-party service providers contracted during the period that were classified by Cloudflare as moderate and high to determine that Cloudflare reviewed the security impact of third-party service providers including third-party attestation reports, security questionnaires, or service provider reported information security controls during the period for each sampled service provider and that action was taken for identified control gaps to address the impact on the organization, if applicable.	No exceptions noted.
CC9.2.3	Agreements containing information security requirements and confidentiality obligations are in place with moderate and high impact third-party service providers.	Inspected agreements in place for a sample of third-party service providers classified by Cloudflare as moderate and high impact to determine that agreements containing information security requirements and confidentiality obligations were in place for each sampled service provider.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	Cloudflare defines availability monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	Inspected the availability monitoring configurations and example ticket for an availability alert generated during the period to determine that Cloudflare defined availability monitoring alert criteria, how alert criteria was flagged, and identified authorized personnel for flagged system alerts.	No exceptions noted.
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Cloudflare's business continuity and disaster recovery plan is reviewed, approved by management, and communicated to relevant team members annually.	Inspected the business continuity and disaster recovery plan to determine that the plan was reviewed, approved by management, and communicated to relevant team members during the period.	No exceptions noted.
A1.2.3	Cloudflare identifies the business impact of relevant threats to assets, infrastructure, and resources that support core business functions.	Inspected the most recent risk assessment performed during the period to determine that Cloudflare identified the business impact of relevant threats to assets, infrastructure, and resources that support core business functions.	No exceptions noted.
A1.2.4	Cloudflare maintains emergency management documentation which is communicated to employees.	Inspected the Cloudflare emergency management page and an e-mail communication related to emergency procedures sent during the period to determine that Cloudflare maintains emergency management documentation which was communicated to employees during the period.	No exceptions noted.
A1.2.5	Cloudflare configures redundant systems and performs daily backups of databases containing customer and end user data to resume system operations in the event of a system failure.	Inspected the database backup and replication configuration and a selected backup log for a database containing end-user or customer data and automated failed backup alert to determine that Cloudflare configured redundant systems and performs daily backups of databases containing customer and end user data to resume system operations in the event of a system failure.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.6	Cloudflare performs backup restoration and failover tests annually to confirm the reliability and integrity of system backups and recovery operations.	Inspected the latest backup restoration and failover test results to determine that Cloudflare performed backup restoration and failover tests annually.	No exceptions noted.
A1.2.7	Cloudflare defines availability monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	Inspected the availability monitoring configurations and example ticket for an availability alert generated during the period to determine that Cloudflare defined availability monitoring alert criteria, how alert criteria was flagged, and identified authorized personnel for flagged system alerts.	No exceptions noted.
AWS and GCP are responsible for implementing controls that ensure the data center facilities are equipped with physical and environmental security safeguards.			
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Cloudflare performs a test of the business continuity and disaster recovery plan annually and ensures the following: <ul style="list-style-type: none"> • Tests are executed with relevant contingency teams • Test results are documented • Corrective actions are taken for exceptions noted • Plans are updated based on results 	Inspected the most recent business contingency and disaster recovery plan test to determine that Cloudflare performed a test of the business continuity and disaster recovery plan during the period and ensured the following: <ul style="list-style-type: none"> • Tests were executed with relevant contingency teams • Test results were documented • Corrective actions were taken for exceptions noted • Plans were updated based on results 	No exceptions noted.

ADDITIONAL CRITERIA FOR CONFIDENTIALITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	Cloudflare has a data classification policy where data classification criteria are reviewed, approved by management, and communicated to authorized personnel at least annually. The data protection officer approves data classification levels and oversees compliance with the data classification policy.	Inspected the data classification policy on the company intranet to determine that Cloudflare had a data classification policy where data classification criteria were reviewed, approved by management, and communicated to authorized personnel during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the data classification policy to determine that the data protection officer approved data classification levels and oversaw compliance with the data classification policy.	No exceptions noted.
C1.1.2	Cloudflare has a data retention policy which establishes guidelines for the minimum and maximum retention periods, including customer and end user data.	Inspected the data retention policy to determine that Cloudflare had a data retention policy which established guidelines for the minimum and maximum retention periods, including customer and end user data.	No exceptions noted.
C1.1.3	Cloudflare performs account and access reviews quarterly and corrective action is taken, when applicable.	Inspected the access review tickets for a sample of quarters during the period to determine that Cloudflare performed account and access reviews for each sampled quarter and that corrective action were taken where applicable.	No exceptions noted.
C1.1.4	Access to modify endpoint utility programs is limited to authorized individuals.	Inspected a system generated listing of users with access to modify endpoint utility programs and their associated job titles with the assistance of the security compliance specialist to determine that access was limited to authorized personnel.	No exceptions noted.
C1.1.5	Break glass actions are logged, and access must be allowed by account admins. Employees with access to make changes to customer accounts are restricted only to authorized personnel.	Inspected the editing permissions, logging configurations, and an example log during the period to determine that break glass actions are logged, and access must be allowed by account admins.	No exceptions noted.
		Inspected a system generated list of user accounts with access to make changes to customer accounts with the assistance of the security compliance specialist to determine that access to make changes to customer accounts was restricted to authorized personnel.	No exceptions noted.
C1.1.6	Customer data is retained for at least 72 hours from the time the data is captured by Cloudflare.	Inspected the data deletion script configuration to determine that customer data was retained for at least 72 hours from the time the data was captured by Cloudflare.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	<p>Cloudflare maintains policies and procedures for the secure handling of media including:</p> <ul style="list-style-type: none"> • Secure access and storage • Secure erasure of media • Secure handling of media • Management of removable media 	<p>Inspected the media protection policy and the hardware recycling process document to determine that Cloudflare maintained policies and procedures for the secure handling of media including:</p> <ul style="list-style-type: none"> • Secure access and storage • Secure erasure of media • Secure handling of media • Management of removable media 	No exceptions noted.
C1.2.2	<p>A data deletion script is configured in the production environment to delete data upon customer request after the expiration of the retention period and in accordance with Cloudflare's internal retention requirements.</p>	<p>Inspected the data deletion script configuration and an example log of deleted customer accounts to determine that a data deletion script was configured in the production environment to delete data upon customer request after the expiration of the retention period and in accordance with Cloudflare's internal retention requirements.</p>	No exceptions noted.