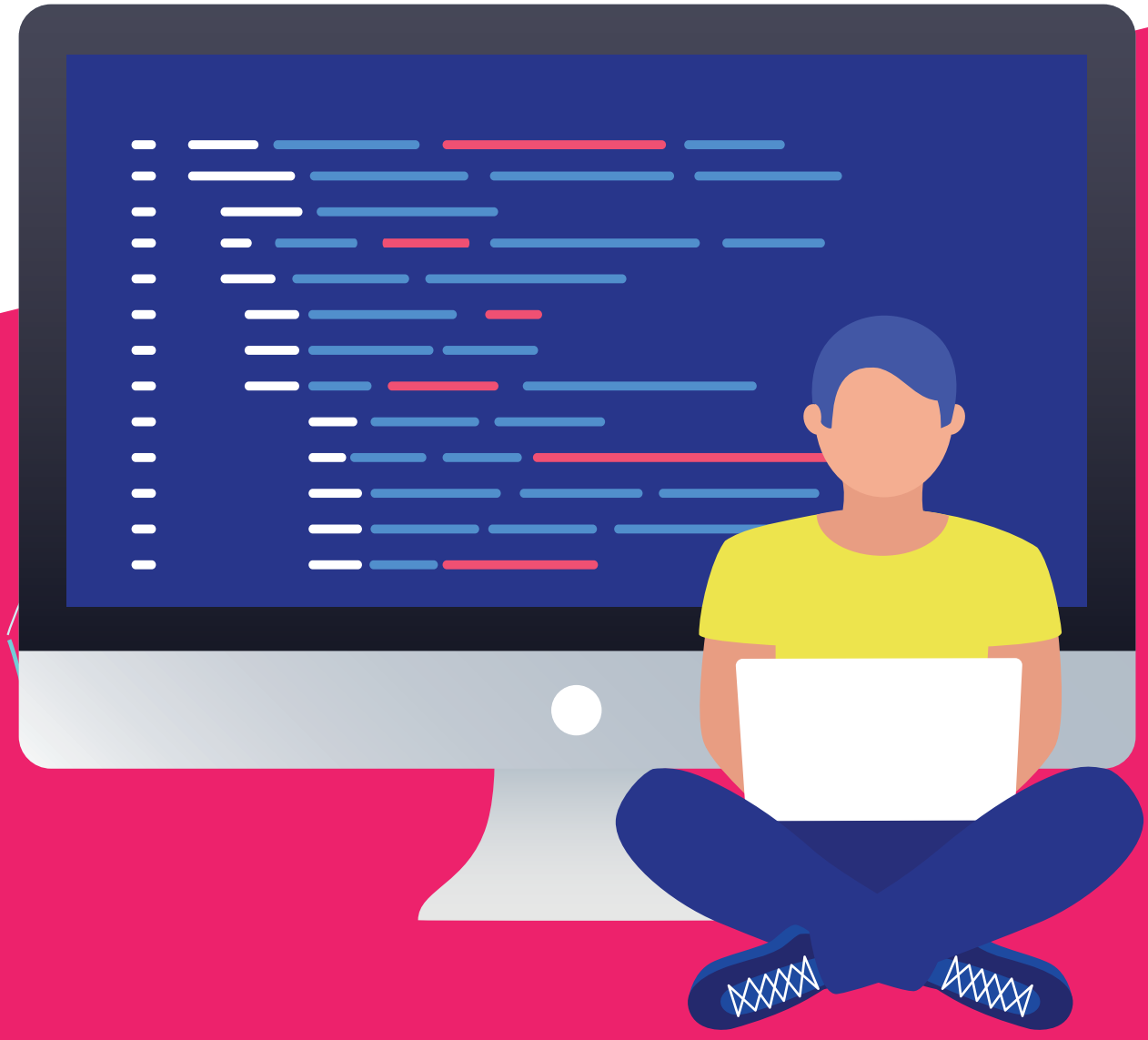
linford&co llp
cpa firm

Codecov



SOC 3

REPORT ON CONTROLS RELEVANT TO SECURITY

MAY 1, 2021 - APRIL 30, 2022

linford&co llp
cpa firm

▪ linford&co llp
1550 wewatta st, 2nd floor
denver, co 80202

▪ tel: +1 (720) 330 7201
email: info@linfordco.com
www.linfordco.com

Section I – Independent Service Auditor's Report

To the Board of Directors of Codecov LLC.:

We have examined Codecov LLC's (Codecov or the Company) accompanying assertion titled, "Assertion of Codecov's Management" (assertion) that the controls within Codecov's code quality improvement services were effective throughout the period May 1, 2021 to April 30, 2022 to provide reasonable assurance that Codecov's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

Our examination included:

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

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Codecov's code quality improvement services were effective throughout the period May 1, 2021 to April 30, 2022, to provide reasonable assurance that Codecov's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

linford&co llp

May 16, 2022
Denver, Colorado

Section II – Assertion of Codecov's Management

May 16, 2022

We are responsible for designing, implementing, operating, and maintaining effective controls within Codecov LLC's (Codecov or the Company) code quality improvement services throughout the period May 1, 2021 to April 30, 2022, to provide reasonable assurance that Codecov's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

We performed an evaluation of the effectiveness of the controls within the system throughout the period May 1, 2021 to April 30, 2022, to provide reasonable assurance that Codecov's service commitments and system requirement were achieved based on the trust services criteria relevant to security (applicable trust service criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Codecov's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented Section III.

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

We assert that the controls within the system were effective throughout the period May 1, 2021 to April 30, 2022, to provide reasonable assurance that Codecov's service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/Jerrod Engelberg
Chief Executive Officer

Section III – Codecov's Description of Its Data Center, Cloud, and Managed Services

Overview of Operations and System Boundaries

Codecov was founded in 2015 with the mission to help clients improve their code review workflow and code quality. Codecov executes its mission by providing a suite of highly integrated code testing tools to group, merge, archive, and compare coverage reports.

Code coverage provides a visual measurement of which source code is being executed by a test suite. This information indicates to a software developer where new tests should be written to achieve higher coverage. Code coverage tools incentivize developers to write tests and increase coverage. During the process of writing tests, a developer may discover new bugs in the source code that need to be resolved before distributing the application.

Codecov takes code coverage to the next level by focusing on integration and promoting healthy pull requests. Codecov delivers coverage metrics directly into the modern workflow to promote more code coverage, especially in pull requests, where new features and bug fixes commonly occur.

The company is headquartered in San Francisco, California and supported by a network of remote employees.

Components of the System Used to Provide the Services

The system used by Codecov to deliver the Codecov code quality improvement services is comprised of a combination of components that include the products and the data processed, but also extends to the underlying infrastructure, subservice organizations' services supporting the platform, the Company's employees and contractors, as well as the policies and procedures followed to maintain the security of the Codecov code quality improvement services and client data. The following is a summary of the components that comprise the system. Specific processes and controls relevant to the security criteria are described in the remainder of this section of the report.

Infrastructure: Codecov uses the subservice organization Google Cloud Platform (GCP) to provide cloud hosting services for its production environment. The facilities, including the hardware and equipment therein, are maintained by the subservice organization. The physical security, environmental control, and incident management for the facilities are also the responsibility of GCP. Codecov is responsible for the configuration and maintenance of its cloud environment. The Company configures firewall protections through security groups and data backups in GCP. GCP undergoes an annual SOC 2 Type II examination, and the report may be obtained directly from them. Codecov obtains and reviews the SOC 2 report provided by GCP related to their hosting operations to determine whether controls are designed and operating

effectively at GCP. Additionally, any listed complementary user entity controls in the GCP SOC report are reviewed and addressed by Codecov.

Security: Codecov has defined its security stance to be one of least privilege and Role Based Access Control (RBAC). Adding new users and removing existing users are performed based on a request ticketing process. In addition, periodic access management audits are performed. Authentication and other access and protective controls have been implemented in order to protect Codecov and client data and information while at rest and while in motion.

Software: The Codecov code quality improvement services are proprietary solutions owned by Codecov. Codecov code quality improvement services are developed and maintained by Codecov's in-house IT and engineering personnel. Codecov follows defined processes to manage changes to the platform.

The processes are designed to mitigate the risks of:

- Corrupted or destroyed information
- Degraded or disrupted computer performance
- Productivity loss
- Introduction of new vulnerabilities, configuration errors, and software bugs in infrastructure and code
- Exposure to reputational risk

Codecov's access to the platform is governed by the principle of least privilege and is limited to authorized personnel. Codecov restricts the ability to implement changes into production to only those individuals who require the ability to implement changes as part of their job function. In addition, Codecov restricts access to Codecov-specific repositories to employee specific accounts registered to the @codecov.io domain.

Monitoring: Codecov has implemented a monitoring, logging, and alerting program. This program includes logging and monitoring for activity related to the:

- Application,
- Infrastructure,
- Security and/or intrusion events, and
- Operational issues.

Identification, notification, resolution, and remediation practices are in place to address the activities when they occur.

People: Codecov personnel are organized into functional areas to facilitate efficient operations and divisions of responsibilities. Codecov provides annual job training to help personnel understand their responsibilities and to maintain security within the organization.

A defined process is followed for the hiring of personnel. This process includes signing an offer letter, having a successful background check completed for those having access to client data, acknowledging Company policies and procedures, and completion of defined security training.

Data: Client data is stored within the Codecov production databases. Codecov has implemented security controls to protect the security of the data. Client data within the databases is encrypted at rest. Additionally, all data transfers between users and Codecov are secured using Transport Layer Security (TLS) and industry-standard encryption.

Processes and Procedures: Codecov maintains security policies and procedures for activities within the organization to maintain the security of the Codecov code quality improvement services. Codecov makes these internal policies and procedures, including security policies, available to its personnel through Vanta, a compliance monitoring tool, to provide direction regarding their responsibilities related to the functioning of internal control. Policies are reviewed regularly and updated as necessary.

Organizational Structure

Management has established structures, reporting lines, and appropriate authorities in the pursuit of Codecov's business objectives. The structures, reporting lines, and authority are clearly communicated through management's operational style, the organizational structure, policies and procedures, and employee job descriptions. Codecov's organizational structure is organized into distinct functions, including Account Management, Engineering, Business Operations, and Finance/Accounting.

Principal Service Commitments and System Requirements

Codecov designs its processes and procedures to meet objectives for its code quality improvement services. Those objectives are based on the service commitments that Codecov makes to user entities and the compliance requirements that Codecov has established for its services.

Security commitments to user entities are documented and communicated in client agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the system are implemented to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Controlled access to the production environment and the supporting infrastructure.
- Segregation of client data.
- Monitoring of system performance metrics and critical application services.

Codecov establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Codecov's policies and procedures,

system design documentation, and contracts with clients. 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 internal networks are managed, and how employees are hired and trained.

(The remainder of this page is left blank intentionally.)