84codes

Report on Controls at a Service Organization Relevant to Security and Availability

SOC 3SM Report

For the Period December 1, 2019 to November 30, 2020

SOC 3 is a registered service mark of the American Institute of Certified Public Accountants (AICPA)

Independent Service Auditor's Report

To the Management of 84codes:

Scope

We have examined 84codes' accompanying assertion titled "Assertion of 84codes Management" (assertion) that the controls its 84codes' system were effective throughout the period December 1, 2019 to November 30, 2020, to provide reasonable assurance that 84codes' service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Service Organization's Responsibilities

84codes 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 84codes' service commitments and system requirements were achieved. 84codes has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, 84codes is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve [Client Short Name]'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 84codes' service commitments and system requirements based on the applicable trust services criteria

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within the 84codes' system were effective throughout the period December 1, 2019 to November 30, 2020, to provide reasonable assurance that 84codes' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

BARR Advisory, P.A.

Fairway, KS

February 4, 2021

Assertion of 84codes Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the 84codes system (system) throughout the period December 1, 2019 to November 30, 2020, to provide reasonable assurance that 84codes' service commitments and system requirements relevant to security and availability were achieved. Our attached system description of the 84codes system identified the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2019 to November 30, 2020, to provide reasonable assurance that 84codes' service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria). 84codes' objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the attached system description.

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 December 1, 2019 to November 30, 2020, to provide reasonable assurance that 84codes' service commitments and system requirements were achieved based on the applicable trust services criteria.

84codes

February 4, 2021

Overview of Operations

Company Background

84codes (the "company"), established in 2012, is a Swedish Aktiebolag headquartered in Stockholm, Sweden. 84codes is dedicated to simplifying cloud infrastructure for developers. The company provides a set of cloud-hosted open source services: CloudAMQP, CloudKarafka, ElephantSQL, and CloudMQTT. 84codes's mission is to help developers focus on building new applications without the worry and effort required to manage their own specialized servers.

Description of Services Provided

84codes provides the following four different Software as a Service (SaaS) solutions:

- *CloudAMQP*: Used to install and manage RabbitMQ clusters. RabbitMQ supports multiple protocols such as advanced message queuing protocol (AMQP), message queuing telemetry transport (MQTT), hypertext transfer protocol secure (HTTPS), simple text oriented message protocol (STOMP), and WebSockets (Web-Stomp). CloudAMQP includes the following features:
    - Fully managed RabbitMQ clusters;
    - Simple monitoring and custom alarms; and,
    - Fast and simple scaling of clusters.
- *CloudKarafka*: Provides the ability to automate every part of setup, running, and scaling of Apache Kafka. CloudKarafka offers hosted publish-subscribe messaging systems in the cloud. With CloudKarafka, customers have a fully managed Kafka cluster up and running within two minutes, including a managed internal Zookeeper cluster on all nodes. CloudKarafka includes the following features:
    - Scaling and upgrading of clusters without downtime;
    - The ability to produce and consume messages over a simple representational state transfer application programming interface (REST API);
    - Kafka Connect provides the ability to integrate Kafka clusters with other systems; and,
    - Managed Zookeeper to track the status of Kafka cluster nodes, topics, and partitions.
- *ElephantSQL:* Automates every part of setup and running of PostgreSQL clusters. Available on all major cloud and application platforms all over the world. ElephantSQL includes the following features:
    - Managed by PostgreSQL experts, with several years of database administration (DBA) experience;
    - Automated backups are included by default, performed daily, and provide the ability to restore a database at a given point in time;
    - Streaming replication across multiple clouds; and,
    - PostgreSQL Browse, which is a browser tool for SQL queries where teams can create, read, update, and delete data directly from a web browser.

- *CloudMQTT:* A hosted message broker for the Internet of Things (IoT). CloudMQTT includes the following features:
    - A pre-configured solution for IoT messaging between low power sensors or mobile devices such as phones, embedded computers, or microcontrollers;
    - Automated setup and running of hosted mosquitto message brokers by 84codes experienced personnel; and,
    - A WebSocket client is used to assist in testing and debugging by providing the ability to display live information from a device or sensor in real time.

84codes's services, described above, automate server configurations and maintenance so customers can focus on building applications instead of taking care of their specialized servers. 84codes also provides 24/7 support in the event customers need support with any of the above services.

Principal Service Commitments and System Requirements

84codes designs its processes and procedures related to the company's system to meet its objectives. Those objectives are based on the service commitments 84codes makes to user entities, the laws and regulations that govern the services provided by 84codes, and the operational and compliance requirements that 84codes has established for the services.

Service commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer 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 designs of the 84codes applications that are designed 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;
- Use of encryption technologies to protect customer data in transit and at rest;
- Patch and vulnerability management procedures, including automatic patching of 84codes servers and scheduled patches for customer servers; and,
- Annual security and compliance awareness training for all 84codes personnel.

Availability commitments include, but are not limited to, the following:

- Regular maintenance that is performed outside peak hours;
- Real-time information and updates on the status of each 84codes service, including uptime reporting via a public-facing webpage for each application that includes the option to subscribe for email updates; and,
- Responses to customer-reported issues through one-to-one communication within 24 business hours.

Such requirements are communicated in 84codes'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 and trained. 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 SaaS services.

Components of the System Used to Provide the Services

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

Infrastructure

A managed network topology and security architecture protects the network from unauthorized external access and segmentation on the internal network. The network topology includes segmented virtual local area networks (VLANs) and access control lists (ACLs). User requests to 84codes's web-based services (CloudAMQP, CloudKarafka, ElephantSQL, and CloudMQTT) are encrypted using Transport Layer Security (TLS) using certificates from an established third party certificate authority. Remote access to virtual hosts is protected via signed keys that require two-factor authentication. The hardware components that make up the aforementioned system include the following:

- **Server hardware:** Server hardware consists of a combination of 84codes-managed infrastructure hosted in multiple AWS data centers for the SaaS platform and managed servers located in AWS's fully managed virtual private cloud which support 84codes's internal systems. Note: 84codes does not have physical access to any of the hardware or servers supporting its services.
- **Network components:** All network components are provided through the cloud providers network interface controllers and firewalls, for example AWS Security Groups. All firewalls are managed in accordance with deny-all policies unless explicitly permitted.

Software

84codes develops and maintains web applications and backend services for provisioning and monitoring servers as well as managing teams, users, subscriptions, and configuration. All internal systems are supported by Amazon Web Services (AWS) products, primarily through Linux servers and PostgreSQL databases.

84codes is responsible for managing the development and operation of the 84codes platform including development and maintenance of infrastructure components such as servers, database and storage systems.

People

84codes's staff consists of approximately 25 employees located worldwide and organized in the following functional areas: Operations, Development, Marketing, Sales & Support, and Compliance & Security.

Data

84codes's information assets are assigned a sensitivity level based on the audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information.

84codes does not know the types of data its customers process, store, or transmit via its services. As such, extreme care and security is taken when handling customers' servers. All data processing is handled as if the data on the customer server could include sensitive information, including personally identifiable information (PII), electronic protected health information (ePHI), etc. Only dedicated team members at 84codes have the ability to access customer data.

The 84codes system provides the ability to delete all content associated with a user account upon request. Customer content is retained and disposed of in accordance with customer agreements and the Data Retention Policy. Once the data is deleted, the software, and its contents, are rendered unreadable systematically.

Processes and Procedures

84codes's Security and Compliance Committee has developed procedures to restrict logical access to the company's systems and protect that information processed, stored, and transmitted through the 84codes system. These procedures are communicated to employees and customers, when applicable. Changes to these procedures are performed annually and authorized by the committee. These procedures cover the following key security life cycle areas:

- Data classification, including data at rest, in motion, and output accuracy;
- Information categorization and classification;
- Assessment of the business impact resulting from proposed security approaches;
- Selection, documentation, and implementation of security controls;
- User access authorization, provisioning, and deprovisioning;
- Monitoring of security controls;
- Maintenance and support of the system, including security-related procedures;
- Backup, recovery, and offline storage;
- Incident response; and,
- System configuration and maintenance, including super user functionality, master passwords, powerful utilities, and boundary protection systems (i.e., AWS Security Groups, firewalls).

Achieving High Security

84codes web applications are only accessible over TLS to safeguard sensitive data during transmission over open, public networks. 84codes internal users are authenticated via G Suite to access 84codes applications. Besides the functional aspects of the site, role-based security is used for 84codes site administration, customer support, and other administration. All data that 84codes holds about its customers is encrypted both at rest and in transit. All data that customers insert to the Service is encrypted at rest per default at 84codes' side (at the cloud platforms that support it). Data in transit can be encrypted by the customer for additional security. Real-time monitoring tools are used to scan the infrastructure for security vulnerabilities and potential security related incidents. AWS Security Groups, or an equivalent in the various cloud providers, are used to restrict ingress and egress traffic to 84codes systems.

Achieving High Scalability

Scalability is of critical importance to 84codes. 84codes follows service-oriented concepts that provide decoupled, modular services. Operating within the various cloud infrastructures allows 84codes to scale services on the fly, both horizontally and vertically. The availability of multiple cloud providers also provides the ability to build additional redundancies in the event a provider is unavailable.

Achieving High Performance

84codes has strict requirements for response times for webpage rendering for the end-user interface. Requirements are achieved by keeping the code algorithmically efficient, reducing the number of layers, and using caching where applicable. At the database layer, high performance is achieved through a data model designed with appropriate indexes to facilitate access patterns. Additionally, regularly scheduled performance tests are analyzed and important architectural decisions are made to ensure that all applications perform at acceptable levels.

Achieving High Availability

High availability is one of the most important architectural considerations at 84codes. In order to help ensure high availability of 84codes services, all services can be deployed across multiple availability zones within each cloud provider. For compute instances that 84codes instantiates and manages, the deployment system manages the multi-AZ deployment. Some services, depending on the cloud provider, provide services that support multi-AZ automatically, such as load balancing which is used where routing is needed to manage access to 84codes applications.

Monitoring Performance, Scalability, and Availability

Performance monitoring at 84codes is done using Statuspage.io, Papertrail, and services within each cloud provider, such as CloudTrail and CloudWatch in AWS. All events are logged and aggregated in Papertrail, which integrates with PagerDuty for real-time alerting and escalations.

Complementary User Entity Controls

84codes controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for 84codes customers, related to the information processed.

For customers to rely on the information processed through 84codes services (applications), each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place.

The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

- User entity is responsible for protecting established user IDs and passwords within their organizations.
- User entity is responsible for reviewing customer access to 84codes applications periodically to validate appropriateness of access levels.
- User entity is responsible for approving and creating new user access to 84codes applications.
- User entity is responsible for removing terminated employee access to 84codes applications.
- User entity is responsible for notifying 84codes if they detect or suspect a security incident related to the 84codes system.
- User entity is responsible for reviewing email and other forms of communications from 84codes related to changes that may affect the 84codes customers and users, and their security or availability obligations.
- User entity is responsible for establishing, monitoring, and maintaining controls over the security for system-generated outputs and reports from the 84codes website.
- User entity is responsible for keeping their RabbitMQ and Erlang versions up to date.
- User entity is responsible for keeping their Apache Kafka version up to date, and following Apache Kafka best practices.
- User entity is responsible for keeping their Mosquitto version up to date, and following Mosquitto best practices.
- User entity is responsible for keeping their PostgreSQL version up to date, and following PostgreSQL best practices.
- User entity is responsible for developing their own disaster recovery and business continuity plans, including architecting the continuity of its systems by choosing the correct plan through 84codes offerings.
- User entity who is HIPAA compliant is responsible for encrypting their data when using 84codes's services.

Complementary Subservice Organization Controls

84codes uses subservice organizations for cloud hosting. These cloud service providers provide physical security and environmental control in support of its 84codes system.

84codes's controls related to the 84codes system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the 84codes system to be achieved solely by 84codes.

Therefore, user entity controls must be evaluated in conjunction with 84codes's controls, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

84codes periodically reviews the quality of the outsourced operations by various methods including:

- Review of subservice organizations' SOC reports; and,
- Non-disclosure agreements.

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	AWS Alibaba Cloud Microsoft Azure DigitalOcean GCP IBM Cloud Rackspace Cloud	CC6.1, CC6.2, CC6.3, CC6.5, 164.312(a)(1), 164.312(a)(2)(i), 164.312(c)(2), 164.312(d)
Physical access to the data center facility is restricted to authorized personnel.	AWS Alibaba Cloud Microsoft Azure DigitalOcean GCP IBM Cloud Rackspace Cloud	CC6.4, CC6.5, 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii)
Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	AWS Alibaba Cloud Microsoft Azure DigitalOcean GCP IBM Cloud Rackspace Cloud	CC6.4, A1.2, 164.310(a)(2)(ii)
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	AWS Alibaba Cloud Microsoft Azure DigitalOcean GCP IBM Cloud Rackspace Cloud	A1.3, 164.308(a)(7)(i), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D), 164.310(a)(2)(i)

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components.	AWS Alibaba Cloud Microsoft Azure DigitalOcean GCP IBM Cloud Rackspace Cloud	A1.2, 164.310(a)(2)(iv)