OneCloud

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the security and availability categories for the period of March 1, 2018 through September 30, 2018.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

ASSERTION OF ONECLOUD MANAGEMENT

ASSERTION OF ONECLOUD MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within OneCloud's SAAS Solution Services System (system) throughout the period March 1, 2018, to September 30, 2018, to provide reasonable assurance that OneCloud's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented in section A and identifies 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 March 1, 2018, to September 30, 2018, to provide reasonable assurance that OneCloud's 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*). OneCloud'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 in section B.

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 March 1, 2018, to September 30, 2018, to provide reasonable assurance that OneCloud's service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

Quin Eddy
CEO and Co-Founder
OneCloud
1460 Broadway
New York, NY 10036

Scope

We have examined OneCloud's accompanying assertion titled "Assertion of OneCloud Management" (assertion) that the controls within OneCloud's SAAS Solution Services System (system) were effective throughout the period March 1, 2018, to September 30, 2018, to provide reasonable assurance that OneCloud's 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

OneCloud is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that OneCloud's service commitments and system requirements were achieved. OneCloud has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, OneCloud 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 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 OneCloud'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 OneCloud'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 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 OneCloud's SAAS Solution Services system were effective throughout the period March 1, 2018, to September 30, 2018, to provide reasonable assurance that OneCloud's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

December 4, 2018

ONECLOUD'S DESCRIPTION OF ITS SAAS SOLUTION SERVICES SYSTEM

SECTION A:
ONECLOUD'S DESCRIPTION OF THE BOUNDARIES OF ITS SAAS SOLUTION SERVICES SYSTEM

Services Provided

The OneCloud Integration Platform as a Service (iPaaS) provides integration and automation between a hybrid mix of on-premise and cloud applications. The multi-tiered platform allows for the creation and management of lightweight and flexible workflows to enable enterprises to quickly connect and integrate their cloud and on-premise applications and systems and supports a managed services approach to integration.

OneCloud provides business users with a web-based automation and orchestration environment, a built-in scheduler, and out-of-the-box functions to streamline automated integration across a heterogeneous stack of applications that co-exist on-premise and in the cloud.

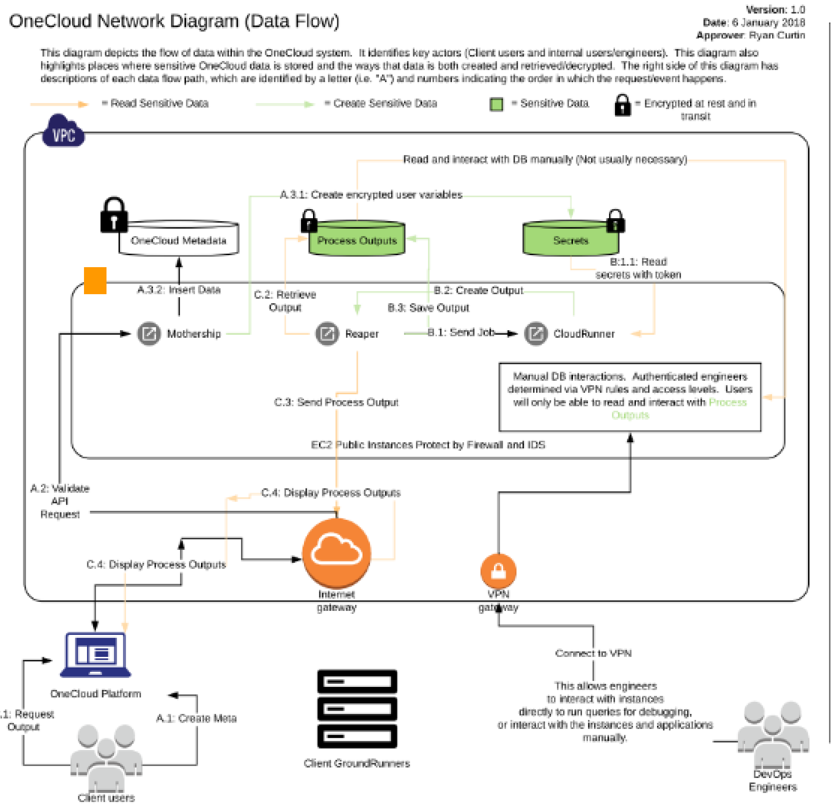
Users interface with the OneCloud host over the HTTPS protocol via web and mobile enabled devices. Running within the OneCloud host is the primary application, an AES encrypted database that securely houses the application metadata as well as a queue to manage communication and task execution on the remote OneCloud service agents. These agents are external to, but controlled by, the core OneCloud host to execute discrete tasks that make up a workflow chain.

OneCloud has been engineered from the ground-up with security, compliance, and control at the heart of its architecture. Leveraging the power of AWS and OneCloud's unique iPaaS architecture, the offering can efficiently integrate and automate cloud and on-premise applications while conforming to comprehensive enterprise architecture standards and strict IT security policies.

Each layer of the OneCloud's architecture is engineered to protect client data and provide access control to the sensitive systems that OneCloud will interface with. Bottom line, OneCloud addresses the requirements of today's modern enterprise architecture while meeting, and in many cases, exceeding the required cloud certifications.

Infrastructure

OneCloud maintains an inventory list of systems including virtual technologies. The CEO is responsible for maintaining physical hardware lists and the CPO maintains the virtual hardware list. To outline the topology of its network, the organization has a network diagram, which is updated every six months or as changes to the architecture occur.


OneCloud Network Diagram (Data Flow)

Version: 1.0
Date: 6 January 2018
Approver: Ryan Curtin

This diagram depicts the flow of data within the OneCloud system. It identifies key actors (Client users and internal users/engineers). This diagram also highlights places where sensitive OneCloud data is stored and the ways that data is both created and retrieved/decrypted. The right side of this diagram has descriptions of each data flow path, which are identified by a letter (i.e. "A") and numbers indicating the order in which the request/event happens.

Manual DB interactions. Authenticated engineers determined via VPN rules and access levels. Users will only be able to read and interact with Process Outputs

This allows engineers to interact with instances directly to run queries for debugging, or interact with the instances and applications manually.

Software

OneCloud maintains a complete inventory of critical software including software license documentation. The organization also develops software. Duties of development/test personnel and production personnel are documented, and code must be tested by a developer other than the code author prior to promotion to the production environment. Testing is performed as part of the Software Development Lifecycle for patches and minor development.

The development/test and production environments are physically separate, which is documented in the environment infrastructure diagram. There are visual distinctions between the production and staging environments, and visual changes as well as naming convention changes are used to reinforce the separation of environments. Staging and production environments exist within different Virtual Private Clouds (VPCs) within the AWS environment.

Source code is stored in and managed with the GitHub version control system. The repositories are actively used to store application code, manage application versions, and restrict access to application code, and only developers have access to the system. Local machines are protected with antivirus, drive encryption, and pre-boot passwords. GitHub is configured with two-factor authentication (2FA).

Applications are protected from vulnerabilities through the use of Open Web Application Security Project (OWASP) secure coding strategies and code review. As previously mentioned, code changes are required to be reviewed by personnel other than the author of the code, and by personnel who are knowledgeable in secure coding practices. Code must be approved prior to promoting code to production.

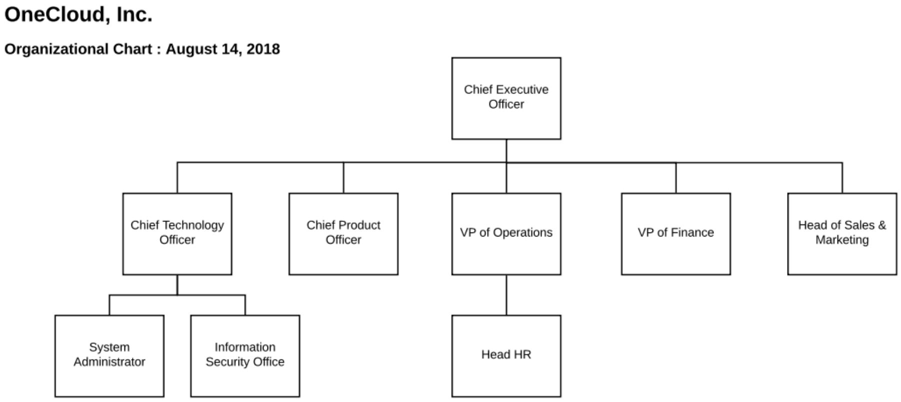
In the event of changes to applications, the organization has application change control procedures in place, which are documented in the Change Management Policy and Application Change Procedure document. Change management workflows have been established and the following are required as part of the change management process:

- Technical specifications developed for significant changes
- Management approval by appropriate parties, along with approval for all stages of the change control lifecycle for each change
- Operational functionality testing performed and documented for each change, where applicable
- Change requests, approved by appropriate departmental management, are received by IT personnel, and recorded

All changes to the production environment, including software related changes, are documented, approved, and tracked.

People

OneCloud has a hierarchical structure, and this structure is outlined in the organization chart.



The organization has a board of directors whose key purpose is to ensure the company's prosperity by collectively directing the company's affairs, while meeting the appropriate interests of its shareholders and stakeholders. The Articles of Incorporation, Corporate Bylaws, and the List of Board members define the roles and responsibilities of the board members.

Data

OneCloud does not store data, but depending on the particular client configuration of OneCloud may or may not transmit and process client data. The movement of sensitive data within the organization’s environment is presented in the network diagram featured in the infrastructure section.

Processes and Procedures

OneCloud has documented security checks that personnel perform that relate to internal security processes. These security checks are documented in the Daily Security Checks document. Checks are completed each morning using a checklist for tasks, and a log of all checks being done is maintained.

SECTION B:
PRINCIPLE SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Contractual Commitments

OneCloud describes the services and scope of work provided to its clients through OneCloud SAAS Subscription Agreements and the organization’s public website. Services and responsibilities are documented and agreed upon by both parties in OneCloud SAAS Subscription Agreements, and contracts must be established before services are provided.

System Design

OneCloud designs its SAAS solution services system to meet its contractual commitments. These commitments are based on the services that OneCloud provides to its clients and the financial, operational, and compliance requirements that OneCloud has established for its services. OneCloud establishes operational requirements in its system design that support the achievement of its contractual commitments. These requirements are communicated in OneCloud’s system policies and procedures, system design documentation, and contracts with clients.