Service Organization Controls 3 (SOC 3) Report

Report on the ControlUp ITOps Analytics and Management Platform Relevant to Security, Availability and Confidentiality

For the Period January 1, 2019 to December 31, 2019

Kost Forer Gabbay & Kasierer
144Menachem Begin Road, Building A
Tel-Aviv 6492102, Israel

Tel: +972-3-6232525
Fax: +972-3-5622555
ey.com

Report of Independent Accountants

To the Management of ControlUp:

We have examined management's assertion that ControlUp, during the period January 1, 2019 to December 31, 2019 maintained effective controls to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification
- the System was available for operation and use, as committed or agreed
- information within the System designated as confidential is protected as committed or agreed

Based on the criteria for security, availability and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100 (2017), Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy. This assertion is the responsibility of ControlUp's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of ControlUp's relevant to security, availability and confidentiality controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.

In our opinion, ControlUp's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability and confidentiality.

The SOC 3 SysTrust for Service Organization or SysTrust Seal on ControlUp's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Very truly yours,

Kost Forer Gabbay and Kasierer

Kost Forer Gabbay and Kasierer
A member firm of Ernst & Young Global
February 1, 2020
Tel Aviv, Israel

Management Assertion on the controls over ControlUp's System based on the AICPA/CICA Trust Services Principles and Criteria for Security, Availability and Confidentiality.

ControlUp maintained effective controls over the security, availability and confidentiality of its ControlUp Information Security Suite (“System”) to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification
- the System was available for operation and use, as committed or agreed
- information within the System designated as confidential is protected as committed or agreed

During the period January 1, 2019 to December 31, 2019, based on the criteria for security, availability and confidentiality in the AICPA’s TSP Section 100, Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy.
Our attached System Description of the System summarizes those aspects of the system covered by our assertion.

Amit Spitzer
Head of Cyber Security & GRC

Amit Spitzer

ControlUp Technologies Ltd.
February 1, 2020

Description of ControlUp ITOps Analytics and Management Platform

Company Overview and Background

ControlUp provides an ITOps analytics and management platform, with a focus on facilitating complex troubleshooting tasks. Used by enterprises worldwide, ControlUp helps ITOps teams to monitor, analyze and remediate problems in their on-premise, cloud and hybrid infrastructure. ControlUp is headquartered in Silicon Valley with R&D in Israel and is backed by Jerusalem Venture Partners and K1 Investment Management.

Products and Services

ControlUp Real-Time – ControlUp Console is used by system administrators for real-time management and monitoring of RDS, VDI, virtual and cloud server environments. The console is responsible for distributing ControlUp agents to the managed computers and offers a UI that enables admins to configure hypervisor connections and monitoring services. The console maintains communication with the relevant managed computers and Hypervisors and display real-time performance data to the sys-admin. The console is also responsible for communicating with ControlUp back-end servers for various operations, and allows for quick identification of performance issues, drilling down to find the root cause within seconds and taking action to troubleshoot any issue using built in management actions and scripts.

ControlUp Insights – ControlUp Insights is analytics and reporting solution that lets system administrators analyze and research historical activity on their virtualization hosts, guest VMs, physical servers, desktops and cloud services. ControlUp Insights collects, stores, correlates, and presents reports on resource utilization metrics, performance and user experience metrics, process activity and user activity metadata. ControlUp Insights also uses anonymized data from hundreds of organizations to create dynamic benchmarks, and utilizes machine learning based algorithms to bring important or unusual findings to the user’s attention, as well as recommend appropriate courses of action when a better alternative is recognized.

Components of the system providing the defined services

ControlUp policies and communication

Formal written policies for the principles and processes within the organization are developed and communicated so that personnel understand ControlUp’s objectives. The assigned policy owner updates the policy annually and the policy is reviewed and approved by the management team. In addition, responsibility and accountability for developing and maintaining the policies are assigned to the ControlUp relevant personnel and are approved on an annual basis by the management team.

Significant components of these policies include, among others:

- Security organizational structure
- Responsibility for information assets
- Information classification and sensitivity
- Access Control
- Reporting
- Security incident response
- Communication Security
- Change management
- Physical security

Communication: ControlUp's Google Apps environment serves as an internal sharing platform for relevant information with ControlUp employees. Access to the Google Apps environment is performed by each employee using its username and password. A system description and its boundaries are documented by the Management team. This document is available to ControlUp customers and prospects via the ControlUp website.

Availability, confidentiality and security related obligations are communicated to ControlUp's employees through the confidentiality and non-disclosure agreements while client obligations and commitments are communicated within the contracts. In addition, on an annual basis, the availability, confidentiality and security-related obligations are communicated to ControlUp employees as part of a security awareness meeting.

Security and Logical Access

Overview

ControlUp has established an information security process designed to protect information at a level commensurate with its value. The access control, user and permissions management are handled as described below.

Production environment – AWS

ControlUp manages and delivers its services using a combination of AWS, which consists of ControlUp production environments. As previously described, information security controls and procedures are implemented throughout these systems, to help prevent unauthorized access to data.

User Permissions and Security groups within AWS

Access to the AWS environment is managed by centralized control. ControlUp new employees are granted access to the ControlUp environment based on their duties and upon approval from the Chief Operations Officer.

Two-factor authentication

Two-factor authentication is implemented for production employee's privileged accounts.

Recertification of Access Permissions

ControlUp has implemented a recertification process to help ensure that only authorized personnel have access to the environments. Users and permissions within the environments are reviewed and approved on a quarterly basis by the Chief Operations Officer.

Revocation Process

In order to assist in the prevention of unauthorized access to data, user accounts within the environments and supporting tools are disabled timely upon termination of employment. Terminated employees complete a termination clearance process on their last day at ControlUp.

Data Segregation - Vulnerability and penetration testing

ControlUp's security program includes testing for security vulnerabilities by an independent security assessment service provider. Penetration tests that help to ensure the overall security status of the ControlUp Information Security Suite, the access to confidential information and consistency with the confidentiality policy are performed. The penetration testing includes, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own.

Security Awareness and Training

In order to help ensure that ControlUp employees are aligned with the security practices and aware of their duties, ControlUp has implemented a security awareness program. The security obligations of users and the entity's security commitments to users are communicated through a security awareness program as well as guidelines as set within the information security policy which are signed by the users.

Security in the Software Development Lifecycle

In order to help ensure the delivery of a highly secure platform, security is an inherent part of the ControlUp Secured Software Development Lifecycle (S-SDLC). Developers undergo secure development and coding practices training and QA engineers undergo security testing and ethical hacking training. The training is given by a leading third party with experience in security, ethical hacking and secure development practices. In addition, regular code review activities are performed as per the software development life cycle (refer to section ' Secured Software Development Lifecycle ("S-SDLC") and Change Management' below).

Secure - Software Development Lifecycle (“S-SDLC”) and Change Management

Software development and Change Management at ControlUp are performed in a manner to help ensure applications are properly designed, tested, approved and aligned with ControlUp clients' business objectives. Several groups are involved in the S-SDLC and Change Management processes. Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented within the ControlUp change management application. In addition, changes that may affect system security, availability or confidentiality related issues are communicated through the change management tool to management and users who will be affected. The S-SDLC process is regularly monitored.

Monitoring

ControlUp’s production environment is monitored by the ControlUp DevOps team. ControlUp has implemented the operations management controls to manage and execute production operations. The availability of the production application is monitored 24/7/365 by the DevOps Team. Key ControlUp staff members are notified of events related to the availability of service to customers.

Support and Operations

ControlUp’s customer support procedures are designed to manage and resolve issues and requests quickly and efficiently. These include issues that are internally identified by ControlUp staff or submitted by customers. ControlUp provides its clients continuous support. Customers report issues through the support team (via Zendesk) and/or their account managers. New employees are trained to use these applications at the beginning of their employment.

Application backup and restore

ControlUp performs and monitors a daily backup - the backup data resides within their respective Cloud Provider’s infrastructure (AWS) and its access is restricted to authorized individuals. Backups of critical customer data including customer configuration data is backed up on a daily basis. The ControlUp infrastructure is programmatically deployed and if the current production systems are unrecoverable then ControlUp can quickly and easily redeploy the entire environment.

Confidentiality Procedures

Customer confidentiality is a key factor in ControlUp. As such, ControlUp has implemented security measures to ensure the confidentiality of its customers sensitive personal information. The security measures aim to prevent unauthorized access, disclosure, alteration or destruction of sensitive personal information. ControlUp access management philosophy is based on least privileged access. In order to make sure that logical access is processed accordingly.

****