Service Organization Controls 3 (SOC 3)

For the Period January 1, 2021 to December 31, 2021

Report on the ControlUp Technologies platform
Relevant to Security, Availability and Confidentiality

Kost Forer Gabbay & Kasierer
144 Menachem Begin St.
Tel-Aviv 6492102, Israel

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

Report of Independent Accountants

To the Management of ControlUp Technologies:

We have examined management's assertion that ControlUp Technologies, during the period November 1, 2020 to October 31, 2021, 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 Technologies'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 Technologies's relevant to security, availability and confidentiality controls.
- (2) Testing and evaluating the operating effectiveness of the controls.
- (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 Technologies's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability and confidentiality.

Very truly yours,

Kost Forer Gabbay and Kasierer

Kost Forer Gabbay and Kasierer
A member firm of Ernst & Young Global
February 1, 2022
Tel Aviv, Israel

Management Assertion on the controls over ControlUp Technologies Platform system, based on the AICPA Trust Services Principles and Criteria for security, availability and confidentiality

We, as management of, ControlUp Technologies Ltd. ("ControlUp Technologies" or " the Company") are responsible for:

- Identifying the ControlUp Technologies System Services and Supporting Services System (system) and describing the boundaries of the system, as presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of our system, as presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the ControlUp Technologies System Services and Supporting Services System (system), to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that the principal service commitments and system requirements were achieved, based on the criteria relevant to security, availability and confidentiality set forth in the AICPA's TSP section 100, 2017 *Trust Services Criteria for Security, Availability, Confidentiality, and Privacy.*

Yours sincerely,

Signature DocuSigned by: Kobi Francis 6830DF885EB1404...

Title GRC Manager

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

Real-Time – ControlUp Real-Time 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.

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.
ControlUp Solve

Solve- ControlUp SOLVE gives powerful, comprehensive, real-time monitoring and analysis in a hosted web application. Accessing ControlUp via a web interface means there's less resource consumption on the endpoints that are logging in and viewing the data, giving the customer and its users a leaner, more performance-driven experience.

Scoutbees - ControlUp Scoutbees monitors the availability and health customer's EUC published resources and various network services (such as HTTP/S, DNS, Ping, etc.) and notifies the customers in advance about any issue in the availability or responsiveness of these resources and services.

Edge DX - ControlUp Edge DX is a cloud-first, scalable platform for managing systems and devices by monitoring and optimizing physical endpoints to provide next-generation user experience and device management.

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.

System Documentation

ControlUp content management application serves as an internal sharing platform for relevant information with ControlUp's employees. The application is available to all ControlUp's employees. The information contained is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components. Each employee is being given a username and password using this application. A description of the ControlUp system and its boundaries is documented and communicated to authorized users through this application. Availability, confidentiality, processing integrity 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, ControlUp's approved policies as well as the process of informing the entity about breaches of the system Security, Availability, Confidentiality and Processing Integrity are communicated to personnel responsible for implementing them in the internal application. ControlUp performs at least annually a security awareness meeting in order to, among others, communicate to ControlUp employees their commitments as it relates to security, availability, and confidentiality.

Risk Assessment

The process of identifying, assessing, and managing risks is a critical component of ControlUp's internal control system. The purpose of ControlUp's risk assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives. Ongoing monitoring and risks assessment procedures are built into the normal recurring

activities of ControlUp and include regular management and supervisory activities. Managers of each department are regularly in touch with personnel and may question the accuracy of information that differs significantly from their knowledge of operations. A risk assessment process is performed on, at least, an annual basis and documented within a dedicated file. And A risk assessment meeting of the management team is performed annually, in order to assess the risks identified and resolution of risks process.

Security, Logical and physical 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 builds its production environment system architecture using AWS's services. Firewall detailed configuration is defined by the ControlUp Operations team and performed either by the ControlUp Operations team or the third-party company. The infrastructure management of the firewalls is performed by the third-party company. The access to the AWS management interface is performed using a two-factor authentication method. In addition, the access to the AWS management interface is restricted to authorized personnel. Moreover, access to the AWS resources is performed through a VPN or from the ControlUp offices. In addition, ControlUp's internal communication network implements a logical segmentation principal, so that network segments are connected through a firewall and not directly to each other. Firewalls separate the internal network from the internet. Firewall settings have been configured to allow only authorized traffic, as defined in ControlUp's Security Policy.

ControlUp manages and delivers its services using a variety of systems and environments. As previously described, information security controls and procedures are implemented throughout these systems, to help prevent unauthorized access to data. Access to system resources is protected through a combination of firewalls, VPNs, native operating system access controls, database management system security, application controls and intrusion detection monitoring software. The database servers reside within the production environment. The access to the production environment servers is restricted to authorized personnel (refer to section 'Production Environment Logical Access). Also, the access to the servers is performed through RDP gateway. External clients are configured at the active directory and are uniquely identified within their own dedicated domain. In addition, a password policy is implemented within the Active Directory.

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, administrators and permissions within the production environment servers and database are reviewed and approved on a quarterly basis by the VP and Director of Operation. Employees whose job functions have changed and therefore no longer require access to a group of user permissions will have their access disabled or modified as needed.

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. A termination ticket is documented, signed, and transmitted to the Human Resources

department. This process includes revocation of access permissions to the systems and premises, as well as the return of the property, data, and equipment.

Physical access

ControlUp recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures and controls have been implemented to help prevent unauthorized access to data, assets, and restricted areas. Physical access to ControlUp office is restricted to authorized personnel using personnel identified card**.** These access cards are issued to ControlUp's employees by the administrative manager. Permissions to issue cards and grant access are restricted to the administrative manager and the authorized designees. In addition, visitors to the ControlUp office are accompanied while on premises**.**

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.

Antivirus and Malicious Software

An antivirus is implemented within the ControlUp servers and within the employee's laptops**.** Anti-virus definition updates are performed and monitored on a regular basis by the IT and Operations teams.

The ability to install applications and software is restricted to authorized individuals. Software is fully controlled before being implemented on the network. Processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software. Antivirus and anti-malware software are implemented and maintained to provide for the interception or detection and remediation of malware. Software that are non-compliant with the company standard are identified and detected. Detection policies and procedures are defined. Detection tools are implemented on Infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities. Anomalies are identified and taken care of by the relevant ControlUp team

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 include the development and production changes to the ControlUp Cloud solutions. The processes are performed in a manner that helps ensure applications are properly designed, tested, approved, and aligned with ControlUp's R&D as well as with ControlUp clients' business objectives and security standards. Several groups are involved in the SDLC and Change Management processes. They are part of the Operations and R&D groups, which defines the change roadmap. Roadmap meetings are performed on a quarterly basis.

Change Initiation: Changes are documented by opening tasks within the change management application. Tasks are prioritized according to their level of urgency and importance by the manager. In addition, weekly change management meeting is performed in order for the VP product to review and approve features. Operation requirements are being taken into consideration when a feature is approved to be developed. The VP operations is in charge of defining the operational needs. First of all, commits performed to the code within the source control are linked to a task within the change management application. Then, a code review is performed and enforced within the source control application. Production bugs are tracked in a dedicated Customer Support portal and the change management application as well. Every bug is assigned to a developer until it is resolved. Once the bug is fixed, the developer updates the bug status within the change management application and the fix is tested by the QA team. Weekly bug meetings are performed in order to discuss and debug the application. Administrative access to the change management application, which allows the creation of builds and the publication of versions, is restricted to authorized personnel. Eventually, a monthly retrospective meeting is performed in order to review the SDLC process.

The QA team is notified to begin the testing according to the workflow within the change management application. Once the task is created, an acceptance test is performed by the QA team or feature owner from the Product team who approves it within the VSTS. Also, prior to moving a change to production, QA is documented and performed using pre-defined test scenarios. Permissions within the VSTS to move tasks from QA to close is restricted to authorized personnel. Additionally, on a weekly basis, a production meeting is performed in order to review the tasks performed the day before and plan the tasks for the current day. The version is then signed-off and transferred by the R&D staff into dedicated environment (QA environment) where another automated testing is running and reviewed by the QA and R&D team leaders. This dedicated environment is not customer-related environment, and its purpose is to determine that the version behaves normally while in an environment similar to the production environment. Once approved, a ticket is opened by the QA representative, and the Operations team deploys the change to the production environment. In fact, builds that went through QA testing successfully can be transferred to the production environment based on approval from the DevOps Manager. Changes to the production environment can only be performed by the DevOps team. Database changes are developed by the developers and tested as part of the QA process (refer to section "QA process" above). Tested database scripts are included within the Change Management Application.

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.

Availability procedures

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.

The backup data captured as part of the daily, weekly, and monthly backup procedures is restored automatically into a separate environment in order to determine the integrity of data and potential data recovery issues. A restore process is performed and documented on an annual basis**.** A log of the restoring process is sent to the Director of Operations for review.

Amazon Web Services provide ControlUp with a secured location implementing security measures to protect against environmental risks or disaster.

Incident Management Process

An incident application is available to ControlUp employees in order to report breaches in system security, availability, and confidentiality**.** New employees are trained in the use of this application at the beginning of their employment. The process is initiated when a new incident is submitted in the Incident Management application or through emails. Incidents are classified according to the level of urgency and importance. Incidents can be submitted into the system following a customer-identified issue, through both manual and automated proactive checks, or automatically through an email request. The application has pre-defined steps that are assigned to a pre-defined group of employees. The completion of each step is recorded in the application. When an incident is submitted an email is sent to the VP of Operations, the Director of Customer Support, and the Operations team. Resources are allocated in order to investigate the incident and resolve the issue. In addition, monthly incident reports are prepared by the Director of Customer Support based on the incident management application information. The reports are sent to the management team for review. The VP of Operations is responsible for escalating critical incidents in the Risk Assessment Meetings. In addition, incident notifications are sent to authorize personnel according to pre-defined rules configured in the monitoring application.

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.

****