SOC 2 Type II Report

For the Period January 1, 2022 to December 31, 2022

REPORT ON CONTROLS PLACED IN OPERATION AT
CONTROLUP TECHNOLOGIES LTD.
RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY
WITH THE INDEPENDENT SERVICE AUDITOR'S REPORT
INCLUDING TEST PERFORMED AND RESULTS THEREOF.

Table of Contents

Section I - ControlUp Technologies Ltd.’s Management Statements

February 15, 2023

We have prepared the accompanying “Description of the ControlUp Platform relevant to Security, Availability and Confidentiality for the period January 1, 2022 to December 31, 2022” (Description) of ControlUp Technologies Ltd (Service Organization) in accordance with the criteria for a description of a service organization’s system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 Report* (Description Criteria). The Description is intended to provide report users with information about the ControlUp Platform (System) that may be useful when assessing the risks from interactions with the System throughout the period January 1, 2022 to December 31, 2022, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for Security, Availability and Confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

ControlUp Technologies Ltd. uses Amazon Web Services to provide Infrastructure Management Services. The Description includes only the controls of ControlUp Technologies Ltd. and excludes controls of the subservice organizations. The Description also indicates that certain trust services criteria specified therein can be met only if complementary subservice organization controls assumed in the design of ControlUp Technologies Ltd.’s controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of the subservice organizations.

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of ControlUp Technologies Ltd’s controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

We confirm, to the best of our knowledge and belief, that:

a. The Description presents the System that was designed and implemented throughout the period January 1, 2022 to December 31, 2022 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls and the subservice organizations applied the controls assumed in the design of ControlUp Technologies Ltd.’s controls throughout the period January 1, 2022 to December 31, 2022.

c. The ControlUp Technologies Ltd. controls stated in the Description operated effectively throughout the period January 1, 2022 to December 31, 2022 to achieve the service commitments and system requirements based on the applicable trust services criteria, if user entities applied the complementary user entity controls and the subservice organizations applied the controls assumed in the design of ControlUp Technologies Ltd.’s controls throughout the period January 1, 2022 to December 31, 2022.

Signature Nofar Danieli

Title GRC Manager

Section II - Independent service auditor's report

The Board of Directors
ControlUp Technologies Ltd.

Scope
We have examined ControlUp Technologies Ltd.'s accompanying "Description of the ControlUp Platform relevant to Security, Availability and Confidentiality for the period January 1, 2022 to December 31, 2022" (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria) and the suitability of the design and operating effectiveness of controls included in the Description throughout the period January 1, 2022 to December 31, 2022 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria for Security, Availability and Confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

ControlUp Technologies Ltd. uses Amazon Web Services (subservice organizations) to provide infrastructure management services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ControlUp, to achieve ControlUp's service commitments and system requirements based on the applicable trust services criteria. The description presents ControlUp's system; its controls; and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and operating effectively at Amazon Web Services. Our examination did not extend to the services provided by Amazon Web Services and we have not evaluated whether the controls management assumes have been implemented at Amazon Web Services have been implemented or whether such controls were suitably designed and operating effectively throughout the period January 1, 2022 to December 31, 2022.

The Description also indicates that ControlUp Technologies Ltd.'s controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of ControlUp's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

ControlUp's responsibilities
ControlUp Technologies Ltd. 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 the service commitments and system requirements were achieved. ControlUp Technologies Ltd. has provided the accompanying assertion titled, "ControlUp Technologies Ltd. Management Assertion" (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. ControlUp Technologies Ltd. is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Service auditor’s responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the Service Organization’s service commitments and system requirements, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed and operating effectively to provide reasonable assurance that the service organization’s service commitments and system requirements would be achieved based on the applicable trust services criteria. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization’s system and the suitability of the design and operating effectiveness of controls involves:

- obtaining an understanding of the system and the service organization’s service commitments and system requirements
- performing procedures to obtain evidence about whether the controls stated in the Description are presented in accordance with the Description Criteria
- performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operating effectively based on the applicable trust services criteria.
- testing the operating effectiveness of those controls based on the applicable trust services criteria.
- evaluating the overall presentation of the Description.

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

Inherent limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs.

Because of their nature, controls at a service organization 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 evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls based on the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in the accompanying Description of Criteria, Controls, Tests, and Results of Tests (Description of Tests and Results).

Opinion

In our opinion, in all material respects:

a. The Description presents the ControlUp Platform system that was designed and implemented throughout the period January 1, 2022 to December 31, 2022 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively [and if the subservice organization and user entities applied the controls assumed in the design of ControlUp's controls throughout the period January 1, 2022 to December 31, 2022.

c. The controls stated in the Description operated effectively to provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period January 1, 2022 to December 31, 2022, if the subservice organization and user entity controls assumed in the design of ControlUp's controls operated effectively throughout the period January 1, 2022 to December 31, 2022.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information, and use of ControlUp, user entities of ControlUp's ControlUp Platform during some or all of the period January 1, 2022 to December 31, 2022 and prospective user entities, independent auditors and practitioners providing services to such user entities who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties, including complementary user entity controls and subservice organization controls assumed in the design of the service organization's controls
- Internal control and its limitations
- User entity responsibilities and how they interact with related controls at the service organization
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Very truly yours,

Kost Forer Gabbay and Kasierer

February 15, 2023
A member firm of Ernst & Young Global
Tel Aviv, Israel

Section III – Description of the ControlUp platform relevant to Security, Availability and Confidentiality for the period of January 1, 2022 to December 31, 2022

Purpose and Scope of the Report

The scope of this report is limited to the controls supporting the ControlUp Application and does not extend to the controls at third-party service providers (e.g. Amazon Web Services)

Note: Parenthetical references have been included in the following narrative as a cross-reference to the applicable control procedures included in the Description of Criteria and Controls section at the end of this report.

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-premises, 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.

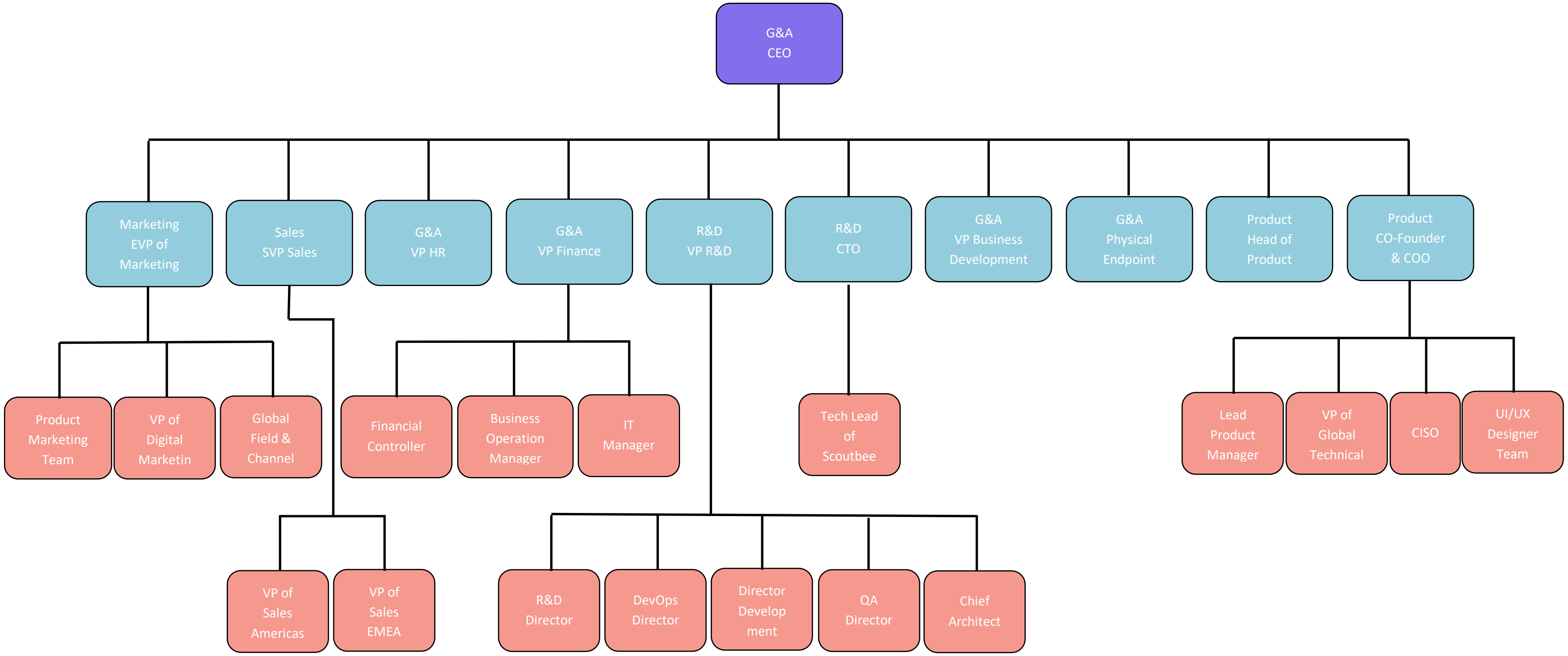
Solve- ControlUp SOLVE gives powerful, comprehensive, real-time monitoring and analysis in a hosted web application. Accessing ControlUp via a web interface means there is less resource consumption on the endpoints that are logging in and viewing the data, giving the customer and its users a leaner,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

Organizational Structure

ControlUp's organizational structure provides the overall framework for planning, directing, and controlling operations. It utilizes an approach whereby personnel and business functions are segregated into departments according to job responsibilities, lines of reporting and communications, and allows employees to focus on the specific business issues impacting their customers. An organization chart is documented and approved by management that clearly defines management authorities and reporting hierarchy (**6**).



Below is a description of key ControlUp departments:
Research: the research department is responsible for seek, explore, and analyze new technologies and solutions for ControlUp's products and services. Under this effort it is also making the first development efforts of new products or major features.

Sales: The sales department is composed of specialized and experienced sales personnel. It is responsible for selling and optimizing sales to ControlUp customers.

Marketing: The marketing department is responsible for building ControlUp's image, generating sales opportunities, and other marketing activities.

IT and Operations: The department includes the following entities:

- Information Technology (IT): The IT department is responsible for providing ControlUp with the required IT environments.
- Cloud Services: The Cloud Services department is responsible for the production SaaS environments availability, security, and scalability. It provides 24x7 control, monitoring, and resolution in case of failure.
- DevOps: The DevOps department works together with R&D during the go-to-live period to deploy the products according to the customer's needs and ControlUp's procedures.

Support: the support team is responsible for providing support to ControlUp's customers. The support team is working closely with Operations, R&D, QA, and Professional Services departments.

Product: The product team is responsible for defining the ControlUp product lines and available services - requirements and priorities. It includes, among others, analyzing market needs and incorporating client's feedback into the products roadmaps.

Research & Development (**R&D**)**:** The R&D department is responsible for developing ControlUp's products and the business services implemented within the production environment. This department includes 3 development teams as detailed below:

- ControlUp RealTime: The ControlUp RealTime development team is responsible for developing the RealTime console application. This includes adding additional content and expanding the feature set. This team is also responsible for improving the architecture of the RealTime console to support large-scale environments.
- ControlUp Insights: The Insights development team is responsible for developing ControlUp's SaaS Insights web portal. This includes integrating additional content and reports to enhance the existing feature set. This team is also responsible for designing the Insights look 'n-feel and improving the user experience and performance.
- Data Team: The Data team is involved in planning and designing the data layer module of ControlUp Insights. The team oversees both application and architecture aspects of the data layer and develops tools and applications to support ControlUp's data lake. This team also develops the Machine Learning algorithms to produce quality insights to our customers.

Quality Assurance (**QA**)**:** The QA department is responsible for testing and validating the R&D's deliverables according to pre-defined scenarios. The QA personnel are integral part of R&D teams and are mentored by the Director of QA overseeing the entire QA activities at ControlUp.

People: System controls are only as strong as the people that implement them. ControlUp commits to employ competent individuals who possess the skills required to successfully implement the company's objectives. Products and services are created and delivered by the company's developers, product and marketing managers, and customer success managers. Members are hired in line with hiring policies and procedures.

Description of the Control Environment, Information Communication, Monitoring and Risk Assessment Processes

A company's internal control is a process – affected by the entity's board of directors, management, and other personnel – designed to enable the achievement of objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations. The following section is a description of the five components of internal control for ControlUp.

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its employees. It reflects the overall attitude, awareness, and actions of management, the Board of Directors, and others concerning the importance of controls and the emphasis given to controls in the entity's policies, procedures, methods, and organizational structure. ControlUp's executive management recognizes its responsibility for directing and controlling operations and for establishing, communicating, and monitoring control policies and procedures. Policy and procedures documents for significant processes that address system requirements and relevant updates are available on the internal intranet.

Authority and Responsibility: Lines of authority and responsibility are clearly established throughout the organization and are communicated through ControlUp's:
(1) Management operating style,
(2) Organizational structure,
(3) Employee job descriptions, and
(4) Organizational policies and procedures.

Board of Directors: There is a Company board that meets on at least a quarterly basis. The board meeting has a fixed agenda. Meeting minutes are retained (**1**)**.** The independent directors are divided into two groups: (1) Industry experts; (2) Investor representatives. The Board of Directors is actively engaged in the governance of ControlUp and its strategic direction. Members of the Board meet on at least a quarterly basis to discuss matters pertinent to ControlUp and to review financial information. The Board's responsibilities include but are not limited to (1) monitoring the actual performance of ControlUp through its financial results; (2) monitoring ControlUp's compliance with legal and regulatory requirements; (3) analysis of the budget vs actual results; (4) guiding ControlUp in the way it funds its operation; (5) approving arrangements with executive officers relating to their employment relationships with ControlUp, including, without limitation, employment agreements, severance agreements, change in control agreements and restrictive covenants and (6) approving equity-based compensation plans in which directors, officers or employees may participate.

Management Philosophy and Operating Style: The Management Team, chaired by the Chief Executive Officer ("CEO"), has been delegated by the Board the responsibility to manage ControlUp and its business on a daily basis. Monthly management meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives (**4**)**.** ControlUp is led by a team with proven ability in media and online customer solution to the global market. In its role, the Management Team assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. The Management Team designs policies and communications so that personnel understand ControlUp's objectives, know how their individual actions interrelate and contribute to those objectives and recognize how and for what they will be held accountable. The Management Team convenes on a monthly basis or more frequently if necessary. In addition, the management Team convenes off-site on a half-year basis for strategic purposes.

Integrity and Ethical Values: Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Integrity and ethical behavior are the products of ControlUp's ethical and behavioral standards, how they are communicated and how they are monitored and enforced in its business activities. They include management's actions to remove or reduce inappropriate incentives or extraneous pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of the organization's values and behavioral standards to personnel through policy statements and from the executives. The Board of Directors and Management Team recognize their responsibility to foster a strong ethical environment within ControlUp to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct.

Human Resources Policy and Practices: Human resource policies and practices relate to hiring, orienting, training, evaluating, promoting, and compensating personnel. Job descriptions are documented and maintained within ControlUp's website. Candidates go through screening and appropriate background checks (**7**)**.** Moreover, new employees are required to sign a standard employment agreement and a Non-Disclosure Agreement addressing business practices, conflicts of interest, confidentiality, and the intellectual property clauses (**2**). The competence and integrity of ControlUp's personnel are essential elements of its control environment. The organization's ability to recruit and retain highly trained, competent, and responsible personnel is dependent to a great extent on its human resource policies and practices. Teams are expected to adhere to the ControlUp's policies that define how services should be delivered and products need to be developed. These are located on ControlUp network and can be accessed by relevant ControlUp team members while communicated by emails on an as-needed basis.

Commitment to Competence: Competence at ControlUp is designed to (1) identify and hire competent personnel, (2) provide employees with the training and information they need to perform their jobs, (3) evaluate the performance of employees to determine their ability to perform job assignments, and (4) through the performance evaluation process, identify opportunities for growth and job performance improvement. Also, new employees go through an onboarding process during which, among others, they are communicated their responsibilities and the different ControlUp's policies (**8**).

Additionally, ControlUp's Team Leaders are responsible for training plans for their newcomers. A professional training for existing employees is typically done only for new tools. It is the manager's role to decide what training a particular employee requires as they relate to specific job requirements. Furthermore, personnel responsible for the design, development, implementation, and operation of systems affecting security, availability and confidentiality undergo training on a regular basis (**9**)**.** An annual review for all employees is taking place. Main review topics are: Job perception, performance feedback, and manager-employee open discussion. Currently this review is not based on quantitative objectives. The review is written and submitted in native language (per site). Salary increases depend on promotion as well as evaluation discussions.

Control Activities

Control activities are the policies and procedures that enable management directives to be carried out to address risks to the achievement of the entity's objectives. ControlUp's operating and functional units are required to implement control activities that help achieve business objectives associated with:
(1) The reliability of financial reporting,
(2) The effectiveness and efficiency of operations and
(3) Compliance with applicable laws and regulations.

The controls activities are designed to address specific risks associated with ControlUp operations and are reviewed as part of the risk assessment process. ControlUp has developed formal policies and procedures covering various operational matters to document the requirements for performance of many control activities.

ControlUp policies relevant to security, availability, and confidentiality

Policies and procedures are documented, reviewed, and approved on an annual basis and available to ControlUp's employees (**3**). 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 designated members of management. Also, a security policy is documented by ControlUp management, reviewed, and approved on an annual basis by the COO and CO-Founder. The security policy is available to ControlUp's employees and reviewed annually within the shared folders (**71**). Security awareness training is performed on an annual basis. A link to the policies and procedures is provided at the end of the meeting (**72**).

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 (**19**)**.** And a risk assessment meeting of the management team is performed annually, in order to assess the risks identified and resolution of risks process (**20**)**.** Moreover, the Company assesses, on an annual basis, the risks that vendors and business partners (and those entities’ vendors and business partners) represent to the achievement of the Company's objectives (**79**).

Risk Mitigation

Once the severity and likelihood of a potential risk has been assessed, management considers how the risk should be mitigated. The mitigation process involves making inferences based on assumptions about the risk and carrying out a cost-benefit analysis. Necessary actions are taken to reduce the level of severity or the likelihood of the risk occurring, and the control activities necessary to mitigate the risk are identified. ControlUp selects and develops control activities that contribute to the mitigation of risks to the achievement of the company’s objectives to acceptable levels. The risk mitigation process is integrated with the company’s risk assessment. Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the Company's objectives during response, mitigation, and recovery efforts (**78**).

Information and Communication

Information and communication are integral components of ControlUp's internal control system. It is the process of identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage and control the organization’s operations. At ControlUp, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees. A detailed system description is documented and available to ControlUp employees within the Company's shared portal (wiki) and to the customers within the ControlUp application (**10**)**.** Senior executives who lead the meetings use information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to organization-wide security policies and procedures are usually communicated to the appropriate ControlUp personnel via email messages and shared with appropriate audience through the use of ControlUp’s Intranet.

Monitoring

Management uses automated reports created through various applications and processes to monitor the efficiency of certain processes and the effectiveness of certain key controls. Metrics produced from these systems are used to identify the strengths and achievements as well as the weaknesses, inefficiencies, or potential performance issues with respect to a particular process. Managers are given the responsibility to inform the individuals who report to them about these items at the appropriate time. The ControlUp Management Team monitors the progress with respect to ControlUp processes on a regular basis. Analysis of root cause is performed through various tools and meetings, and corrective measures are communicated to relevant groups through emails, meetings, and a project portal tool in order to prevent future occurrences.

Asset Management

Company assets are tracked and managed throughout the asset lifecycle. Assets are assigned owners to ensure there is an individual responsible for securing the asset. The tracked assets include production components as well as employee devices that may contain personal data. When assets reach end of life, they are securely destroyed to ensure that data is not recoverable.

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.

Communication

ControlUp content management application serves as an internal sharing platform for relevant information with ControlUp's employees. Each employee is being given a username and password using this application. In addition, ControlUp's approved policies as well as the process of informing the entity about breaches of the system Security, Availability and Confidentiality are communicated to personnel responsible for implementing them in the internal application. Changes impacting customers are reviewed in a go/no-go meeting and communicated through release note through the company website (**14**)**.** Moreover, new features are communicated to customers, if relevant, through the website. The release notes are available to the client (**18**)**.**

Logical and Physical Access

ControlUp has established an organization-wide information security policy designed to protect information at a level commensurate with its value. The policy dictates security controls for media where information is stored, the systems that process it, as well as infrastructure components that facilitate its transmission. That including, strong password configuration settings are enabled on the internal ControlUp domain using Group Policies. These settings include: (1) forced password change at defined intervals; (2) a minimum password length; (3) a limit on the number of unsuccessful attempts to enter a password before the user ID is suspended; and (4) password complexity requirements (**30**)**.**

Access Control, User and Permissions Management

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 (**24**)**.** In addition, the access to the AWS management interface is restricted to authorized personnel (**25**)**.** Moreover, access to the AWS resources is performed through a VPN or from the ControlUp offices (**29**)**.** 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 (**39**)**.** 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 (**26**)**.** External clients are configured at the active directory and are uniquely identified within their own dedicated domain (**33**)**.** In addition, a password policy is implemented within the Active Directory (**27**)**.**

Recertification of Access Permissions

ControlUp has implemented a recertification process to help ensure that only authorized personnel have access to the production interface, servers, environments, and databases. Users, administrators and permissions within the production environment servers and database are reviewed and approved on a semi-annual basis by the VP and Director of Operation (**35**)**.**

Employees are provided with the minimal access rights required to carry out their duties. However, new users accessing ControlUp system are granted access upon notification from the HR department. A detailed ticket is opened in the IT management ticketing system using a new hire template (**32**). The template includes all user detailed permissions including the team the new employee belongs to. This membership defines permissions and access granted to the new employee.

Revocation Process

In order to assist in the prevention of unauthorized access to data, user accounts within the ControlUp production environment and supporting tools are disabled promptly upon termination of employment. Terminated employees go through an off-boarding process and if they had access to the production environment, they have their permissions removed in a timely manner (**31**)**.** 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.

Software Development Lifecycle (SDLC) Overview

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 (**5**)**.**

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 (**48**)**.** In addition, weekly change management meetings are performed in order for the VP product to review and approve features (**49**)**.** Operation requirements are being taken into consideration when a feature is approved to be developed. The VP operations are in charge of defining the operational needs (**46**)**.** First of all, commits performed to the code within the source control are linked to a task within the change management application (**53**)**.** Then, a code review is performed and enforced within the source control application (**62**)**.** 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 (**58**)**.** 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 (**59**)**.**

Software Testing and QA 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 (**51**)**.** Also, prior to moving a change to production, QA is documented and performed using pre-defined test scenarios (**55**)**.** Permissions within the VSTS to move tasks from QA to close are restricted to authorized personnel (**52**)**.** 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 (**50**)**.** 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 (**56**)**.** Changes to the production environment can only be performed by the DevOps team (**61**)**.** 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.

ControlUp’s production environment

The processes described below are executed within ControlUp's production environment, hosted in co-location data centers by a third-party vendor. Amazon Web Services in the United States (N. Virginia) and Europe (Ireland)),

AWS: ControlUp's infrastructure runs on top of AWS’s Infrastructure as a Service (IaaS) and utilizes various services such as: (1) EC2, (2) S3, (3) RDS (4), Redshift, (5) EMR, (6) CloudFront, which is the AWS’s CDN, and more. These services are designed to make web-scale computing easier for ControlUp.

AWS’s web service interface (AWS Console) allows ControlUp to obtain and configure capacity. It provides ControlUp with control of computing resources and runs on AWS’s computing environment. Ec2 reduces the time required to obtain and boot new server instances to minutes, allowing to quickly scale capacity, both up and down, as computing requirements change. The use of EC2 allows to:

- Select a pre-configured template to get up and running immediately or create a per-need AMI containing ControlUp-configured applications, libraries, data, and associated configuration settings.
- Configure security and network access on the Ec2 instance.
- Choose which instance type(s), then start, terminate, and monitor as many instances as needed, using the web service APIs.
- Determine whether to run in multiple locations, utilize static IP endpoints, or attach persistent block storage to instances.

Production Environment Logical Access

Several controls are in place to insure that logical access processes are performed according to the industry best practice:

- Single sign-on (SSO) is used for identity and access management (IAM) that enables users to securely authenticate with multiple applications and websites by logging with one set of credentials. The application relies on a trusted third party to verify the users (**75**).

- The access to the production server is performed using a two-factor authentication method and through an email approval from the DevOps and is restricted to authorized personnel (**23**).
- Developers do not have direct access to the production and database environment. The access is reviewed on a yearly basis. Specific developers have access and log of actions are reviewed (**57**).
- Access to sensitive permissions within the build tool is restricted authorized personnel (**74**).
- Database changes are performed using pre-approved scripts (**60**).
- The access to the offline storage, backup data, systems and media is restricted to authorized individuals (**34**).

Remote Access

ControlUp’s internal networks are protected using commercial firewalls configured and administered by the IT department. In addition, ControlUp’s production environment servers are protected by the AWS’s tools and controls implemented by. Traffic entering ControlUp’s production network is monitored and screened by a firewall and monitoring tools implemented by AWS. Remote users are automatically disconnected from the production servers after a pre-defined period of inactivity and need to login again in order to re-establish connection to the network. ControlUp implemented a GPO policy that locks its servers after twenty minutes of inactivity. The AWS console configuration requires the user to login every twelve hours.

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's office is restricted to authorized personnel using a personal identified card (**37**)**.** 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 (**38**)**.**

Data Centers

Production environment physical security is managed by Amazon Web Services. In fact, ControlUp employees do not have access to neither the N. Virginia data centers nor the Ireland data centers. Our cloud providers are responsible for implementing an appropriate set of controls in order to address physical security issues.

ControlUp performs a review of the SOC 2 report of its datacenter on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at ControlUp to address the CUECs (**82**).

Penetration Testing

Penetration tests that help ensure the overall security status of the production platform and consistency with the confidentiality policy are performed on an annual basis (**43**)**.** The penetration tests include, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own. Also, a vulnerability scan is performed on a quarterly basis using an automated external tool (**45**)**.**

Antivirus

An antivirus is implemented within the ControlUp servers and within the employee's laptops (**42**)**.** Anti-virus definition updates are performed and monitored on a regular basis by the IT and Operations teams.

Infrastructure Change Management Overview

ControlUp regularly makes changes within its production environment in response to the evolving client and market needs. These changes include adding/removing/changing the configuration policies of the existing servers or performing routine maintenance activities, software updates, and other infrastructure-related changes accordingly to available possibilities provided by the third-party vendors. Infrastructure changes are documented within the Change Management tool. The request is reviewed and approved by the Director of Operations**.**

Emergency changes: Emergency changes are performed and updated as part of hot fixes, which follow the same process as described above though the timeframe may be shortened, and approvals may be provided after the change was already performed.

Monitoring the Change Management Process

A risk assessment meeting of the management team is performed every six months, in order to assess the risks identified and review changes performed to the application. Action items are updated within the ControlUp management tool.

Malicious software

The ability to install applications and software is restricted to authorized individuals. Software are 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 is 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.

Availability Procedures

ControlUp's production environment is fully managed as part of AWS' services and monitored by ControlUp Operation team using the tools provided by the third-party vendors as well as internal tools. The application level is fully managed by the ControlUp Operations team. ControlUp's application database and critical portions of the application file system are backed up incrementally on a daily basis (**64**)**.** Additionally**,** application backup is performed on a daily basis. Alerts are sent if the backup fails (**63**)**.** ControlUp has implemented the operations management controls described below to manage and execute production operations. ControlUp's databases are hosted at AWS.

Database Backup

ControlUp's databases are hosted at AWS. Snapshots of the servers are performed on a daily basis. Alerts are sent if the backup fails (**65**)**.** The access to the database is restricted to authorized personnel (**28**)**.** In addition, database disks are encrypted using the AWS service using a KMS key. ControlUp end-point disks are encrypted as well (**68**)**.** ControlUp databases are replicated to multi availability zones (**80**).

Restoration

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 (**66**)**.** A log of the restoring process is sent to the Director of Operations for review. In addition, ControlUp has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of a disaster (**81**).

Data Center Availability Procedures

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

Production Monitoring

ControlUp's production network encompasses numerous components including web services, application and data server types, database, monitoring tools, and redundant network equipment provided as part of AWS' services. In addition, in order to improve service availability to clients and to support the operations of the ControlUp environments, ControlUp maintains a dedicated Operations department. The Operations department is responsible for the ongoing work on the production environment as well as investigating escalated issues. The production environment, including the servers and application, is monitored 24/7/365 by the NOC and Operations team. Key ControlUp staff is notified of events related to the security, availability, or confidentiality of service to clients (**22**)**.** ControlUp uses a suite of monitoring tools in order to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules (**21**)**.** Also, applicative anomalies are identified using pre-defined rules on a monitoring tool (**44**)**.**

In addition, actions performed on the production environment, including OS, DB and application are monitored and logged. This log is reviewed on a monthly basis by the dedicated personnel and alerts are triggered upon the identification of an anomaly (**76**).

Incident Management Process

The company has developed an Incident Management Process in order to respond to Security Incidents and Personal Data Breaches in accordance with applicable laws and regulations (**77**). An incident application is available to ControlUp employees in order to report breaches in system security, availability, and confidentiality (**47**)**.** 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.

Support

ControlUp's customer support procedures are designed to handle and resolve issues and requests in a timely manner. This includes issues that are internally identified, or issues submitted by clients. ControlUp provides its clients with three types of support. ControlUp customers choose either the Standard support level, Premium support level or Customized support level (as per customer request). All three types are available 24/7/365 via support mail, support hotline and customer support portal. The main difference between these three types is the response time. All types are handled by ControlUp according to the Service Level Agreement procedure. As well as a how-to is available in order to guide the customer in how to use the product (**11**)**.**

Ticketing and Management

ControlUp opens a ticket when an issue is raised by a client or when an issue is proactively identified. ControlUp uses a third-party CRM application to manage, classify and ticket the client support-related issues. Tickets are classified by the level of urgency and assigned to the appropriate support tier for resolution (**15**)**.** The SLA procedures are documented and available to customers on the company website. Tickets are classified and assigned to the relevant queue, handled by a dedicated support team. The issues are documented within the CRM tool (**12**)**.**

Escalation Process

ControlUp's goal is to resolve issues in an efficient manner. The issue is tracked and updated in the CRM system. The escalation process is defined and documented by Customer Support. Tickets are escalated as deemed necessary to Operations, R&D or Professional Services teams. Service interruptions, maintenance and updates are communicated to customers through the company website (**73**). Support meetings with the management are performed on at least a monthly basis, in order to report major open issues to the management (**16**)**.** In addition, to maintain visibility on current support issues and potential problem trends, support metrics (including Key Performance Indicators) are generated from the CRM application and sent to Company's stakeholders on a monthly basis (**17**)**.**

Monitoring

The management team is updated on a weekly basis on security, confidentiality and availability non-compliance issues that may come up, and address them as needed. Such issues are documented as part of an RCA (Root Cause Analysis) report created by the Support team, the Operations team, or the VP of Operations. Change reports from the Change Management Tool, vulnerability reports from production and monitoring tools as well as support metrics are reviewed and discussed in relation to organization's system security, availability, processing integrity and confidentiality policies. In addition, environmental, regulatory, and technological changes are monitored. Their effects are assessed, and their policies are updated accordingly. A summarized protocol is made available to relevant managers and team members.

Confidentiality Procedures

Customer confidentiality is key factor in ControlUp. As such, ControlUp has implemented security measures to ensure the confidentiality of its customer's sensitive personal information. Confidentiality agreement is disclaimed as it relates to contracts with infrastructure third party providers in accordance with ControlUp confidentiality policy (**70**)**.** Customers' passwords, sensitive information and PII encrypted within the ControlUp application database according to the ControlUp security policy (**40**)**.** Application server disks are encrypted when available and deemed necessary by ControlUp (**69**)**.** In addition, connections to the ControlUp network and databases are obtained through a secured IPSEC tunnel, only accessible from within the production network. Clients' sessions and interactions are encrypted using 256bit SSL V3/TLS HTTPS (**67**)**.** Internet traffic is encrypted using high class level certificates based on the PKI infrastructure.

Subservice Organization carved out controls: Amazon Web Services (AWS)

The subservice organization is expected to:

- Implement controls to enable security and monitoring tools within the production environment.
- Implement logical access security measures to infrastructure components including native security or security software and appropriate configuration settings.
- Restrict the access to the virtual and physical servers, software, firewalls, and physical storage to authorized individuals and to review the list of users and permissions on a regular basis.
- Implement controls to:
    - Provision access only to authorized persons.
    - Remove access when no longer appropriate.
    - Secure the facilities to permit access only to authorized persons.
    - Monitor access to the facilities.
- Be consistent with defined system security as it relates to the design, acquisition, implementation, configuration modification, and management of infrastructure and software.
- Maintain system components, including configurations consistent with the defined system security, related policies.
- Provide that only authorized tested and documented changes are made to the system.

ControlUp's customers' responsibilities

- Implementing sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with ControlUp.
- Ensuring timely removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with ControlUp's services.
- Maintaining authorized, secure, timely, and complete transactions for user organizations relating to ControlUp's services.
- Protecting data that is sent to ControlUp by using appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.
- Implementing controls requiring additional approval procedures for critical transactions relating to ControlUp's services.
- Reporting to ControlUp in a timely manner any material changes to their overall control environment that may adversely affect services being performed by ControlUp.
- Notifying ControlUp in a timely manner of any changes to personnel directly involved with services performed by ControlUp. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by ControlUp.
- Adhering to the terms and conditions stated within their contracts with ControlUp.
- Developing, and if necessary, implementing a business continuity and disaster recovery plan (DRP) that will aid in the continuation of services provided by ControlUp.

Section IV - Description of Criteria, Controls, Tests and Results of Tests

Testing Performed and Results of Tests of Entity-Level Controls

In planning the nature, timing and extent of its testing of the controls specified by ControlUp, KFGK considered the aspects of ControlUp control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE, including Electronic Audit Evidence (EAE) (e.g., controls requiring system-generated populations for sample-based testing), we performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspect the source of the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) tie data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity. In addition to the above procedures, for tests of controls requiring management’s use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), we inspected management’s procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Criteria and control

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by, and are the responsibility of ControlUp. The testing performed by Kost Forer Gabbay and Kasierer (KFGK) and the results of tests are the responsibility of the service auditor.

Control Environment

CC1.1 / COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	New employees are required to sign a standard employment agreement and a Non-Disclosure Agreement addressing business practices, conflicts of interest, confidentiality and the intellectual property clauses.	Inspected the signed employment agreement for a sample of new employees and determined the agreement included confidentiality and intellectual properly clauses.	No deviations noted.
7	Job descriptions are documented and maintained within ControlUp's website. Candidates go through screening and appropriate background checks.	Inspected ControlUp’s website and determined that job descriptions were documented and maintained within ControlUp's website. For a sample of employees, inspected the hiring process checklists and determined that candidates went through screening and appropriate background checks.	No deviations noted.

CC1.2 / COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	There is a Company board that meets on at least a quarterly basis. The board meeting has a fixed agenda. Meeting minutes are retained.	Inspected a sample of meeting minutes and invitations and determined that board meetings were performed on at least a quarterly basis. The board meeting had a fixed agenda. Meeting minutes were retained	No deviations noted.

CC1.3 / COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	There is a Company board that meets on at least a quarterly basis. The board meeting has a fixed agenda. Meeting minutes are retained.	Inspected a sample of meeting minutes and invitations and determined that board meetings were performed on at least a quarterly basis. The board meeting had a fixed agenda. Meeting minutes were retained	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	New employees are required to sign a standard employment agreement and a Non-Disclosure Agreement addressing business practices, conflicts of interest, confidentiality and the intellectual property clauses.	Inspected the signed employment agreement for a sample of new employees and determined the agreement included confidentiality and intellectual properly clauses.	No deviations noted.
3	Policies and procedures are documented, reviewed and approved on an annual basis and available to ControlUp's employees.	Inspected the policies and determined that policies were documented, reviewed and approved by management on an annual basis. Inspected the internal portal and determined that policies were available to employees.	No deviations noted.
4	Monthly management meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls and other strategic initiatives.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a monthly basis and that meeting minutes were retained.	No deviations noted.
5	Roadmap meetings are performed on a quarterly basis.	Inspected a sample of Roadmap meeting invitations and determined that they were performed on a quarterly basis.	No deviations noted.
6	An organization chart is documented and approved by management that clearly defines management authorities and reporting hierarchy.	Inspected the company's organization chart and determined that it was documented and approved by management. The organization chart clearly defined management authorities and reporting hierarchy.	No deviations noted.

CC1.4 / COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
7	Job descriptions are documented and maintained within ControlUp's website. Candidates go through screening and appropriate background checks.	Inspected ControlUp's website and determined that job descriptions were documented and maintained within ControlUp's website. For a sample of employees, inspected the hiring process checklists and determined that candidates went through screening and appropriate background checks.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
8	New employees go through an onboarding process during which, among others, they are communicated their responsibilities and the different ControlUp's policies.	Inspected the onboarding checklists for a sample of new employees and determined that new employees went through an onboarding process during which, among others, were communicated their responsibilities and the different ControlUp policies.	No deviations noted.
9	Personnel responsible for the design, development, implementation, and operation of systems affecting security, availability and confidentiality undergo training on a regular basis.	Inspected ControlUp's training program and determined that training was performed on an ad-hoc basis by R&D personnel.	No deviations noted.
72	Security awareness training is performed on an annual basis. A link to the policies and procedures is provided at the end of the meeting.	Inspected the security awareness training documentation and determined that security awareness training was performed on an annual basis. A link to the policies and procedures was provided at the end of the meeting.	No deviations noted.

CC1.5 / COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
6	An organization chart is documented and approved by management that clearly defines management authorities and reporting hierarchy.	Inspected the company’s organization chart and determined that it was documented and approved by management. The organization chart clearly defined management authorities and reporting hierarchy.	No deviations noted.
8	New employees go through an onboarding process during which, among others, they are communicated their responsibilities and the different ControlUp's policies.	Inspected the onboarding checklists for a sample of new employees and determined that new employees went through an onboarding process during which, among others, were communicated their responsibilities and the different ControlUp policies.	No deviations noted.
9	Personnel responsible for the design, development, implementation, and operation of systems affecting security, availability and confidentiality undergo training on a regular basis.	Inspected ControlUp's training program and determined that training was performed on an ad-hoc basis by R&D personnel.	No deviations noted.

Communication and Information

CC2.1 / COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
10	A detailed system description is documented and available to ControlUp employees within the Company's shared portal (wiki) and to the customers within the ControlUp application.	Inspected the description of the ControlUp system and its boundaries and determined that it was available to ControlUp employees within the Company's shared portal (wiki). Inspected the description of the ControlUp system and its boundaries and determined that it was available to the customers within the ControlUp application.	No deviations noted.
71	A security policy is documented by ControlUp management, reviewed and approved on an annual basis by the COO and CO-Founder. The security policy is available to ControlUp's employees and reviewed annually within the shared folders.	Inspected the company security policy and determined that a security policy was documented by ControlUp management, reviewed and approved on an annual basis by the COO and CO-Founder. Inspected the company's shared folders and determined that the security policy was available to ControlUp's employees within the shared folders.	No deviations noted.
20	A risk assessment meeting of the management team is performed annually, in order to assess the risks identified and resolution of risks process	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key ControlUp stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were documented.	No deviations noted.

CC2.2 / COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	New employees are required to sign a standard employment agreement and a Non-Disclosure Agreement addressing business practices, conflicts of interest, confidentiality and the intellectual property clauses.	Inspected the signed employment agreement for a sample of new employees and determined the agreement included confidentiality and intellectual properly clauses.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3	Policies and procedures are documented, reviewed and approved on an annual basis and available to ControlUp's employees.	Inspected the policies and determined that policies were documented, reviewed and approved by management on an annual basis. Inspected the internal portal and determined that policies were available to employees.	No deviations noted.
4	Monthly management meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls and other strategic initiatives.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a monthly basis and that meeting minutes were retained.	No deviations noted.
5	Roadmap meetings are performed on a quarterly basis.	Inspected a sample of Roadmap meeting invitations and determined that they were performed on a quarterly basis.	No deviations noted.
8	New employees go through an onboarding process during which, among others, they are communicated their responsibilities and the different ControlUp's policies.	Inspected the onboarding checklists for a sample of new employees and determined that new employees went through an onboarding process during which, among others, were communicated their responsibilities and the different ControlUp policies.	No deviations noted.
10	A detailed system description is documented and available to ControlUp employees within the Company's shared portal (wiki) and to the customers within the ControlUp application.	Inspected the description of the ControlUp system and its boundaries and determined that it was available to ControlUp employees within the Company's shared portal (wiki). Inspected the description of the ControlUp system and its boundaries and determined that it was available to the customers within the ControlUp application.	No deviations noted.
12	The SLA procedures are documented and available to customers on the company website. Tickets are classified and assigned to the relevant queue, handled by a dedicated support team. The issues are documented within the CRM tool.	Inspected the Master Service Agreement that included the SLA and determined that the SLA procedures were documented and available to customers on the company website.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the CRM tool and determined that tickets were classified and assigned to the relevant queue, handled by a dedicated support team. The issues were documented within the CRM tool	
71	A security policy is documented by ControlUp management, reviewed and approved on an annual basis by the COO and CO-Founder. The security policy is available to ControlUp's employees and reviewed annually within the shared folders.	Inspected the company security policy and determined that a security policy was documented by ControlUp management, reviewed and approved on an annual basis by the COO and CO-Founder. Inspected the company's shared folders and determined that the security policy was available to ControlUp's employees within the shared folders.	No deviations noted.
15	ControlUp uses a third-party CRM application to manage, classify and ticket the client support-related issues. Tickets are classified by the level of urgency and assigned to the appropriate support tier for resolution.	Inspected a sample of client issues and determined that a CRM tool was used in order to manage client tickets. Tickets were prioritized according to the importance.	No deviations noted.
16	Support meetings with the management are performed on at least a monthly basis, in order to report major open issues to the management.	Inspected a sample of support meeting invitations and determined that support meetings were performed on a monthly basis in order to report major open issues to the management.	No deviations noted.
17	Support metrics (including Key Performance Indicators) are generated from the CRM application and sent to Company’s stakeholders on a monthly basis.	Inspected a sample of KPI reports generated from the CRM application and determined that support metrics (including Key Performance Indicators) were generated from the CRM application and sent to Company’s stakeholders on a monthly basis.	No deviations noted.

CC2.3 / COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Monthly management meetings are held to discuss operational efficiencies within the applicable	Inspected a sample of management meeting minutes and invitations and determined that the management	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	functional areas and to disseminate new policies, procedures, controls and other strategic initiatives.	met on a monthly basis and that meeting minutes were retained.	
10	A detailed system description is documented and available to ControlUp employees within the Company's shared portal (wiki) and to the customers within the ControlUp application.	Inspected the description of the ControlUp system and its boundaries and determined that it was available to ControlUp employees within the Company's shared portal (wiki). Inspected the description of the ControlUp system and its boundaries and determined that it was available to the customers within the ControlUp application.	No deviations noted.
11	A how-to is available in order to guide the customer in how to use the product.	Inspected the company website and observed that a how-to was available in order to guide the customer in how to use the product.	No deviations noted.
12	The SLA procedures are documented and available to customers on the company website. Tickets are classified and assigned to the relevant queue, handled by a dedicated support team. The issues are documented within the CRM tool.	Inspected the Master Service Agreement that included the SLA and determined that the SLA procedures were documented and available to customers on the company website. Inspected the CRM tool and determined that tickets were classified and assigned to the relevant queue, handled by a dedicated support team. The issues were documented within the CRM tool	No deviations noted.
14	Changes impacting customers are reviewed in a go/no-go meeting and communicated through release note through the company website	Inspected a sample of go/no-go meeting minutes and determined that changes impacting customers were reviewed and communicated through release note emails where applicable.	No deviations noted.
15	ControlUp uses a third-party CRM application to manage, classify and ticket the client support-related issues. Tickets are classified by the level of urgency and assigned to the appropriate support tier for resolution.	Inspected a sample of client issues and determined that a CRM tool was used in order to manage client tickets. Tickets were prioritized according to the importance.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
73	Service interruptions, maintenance and updates are communicated to customers through the company website	Inspected the ControlUp status page and determined that Service interruptions, maintenance and updates were communicated to customers through the company website	No deviations noted.

Risk Assessment

CC3.1 / COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
19	A risk assessment process is performed on, at least, an annual basis and documented within a dedicated file.	Inspected the risk assessment documentation and determined that a risk assessment process was performed on, at least, an annual basis and documented within a dedicated file.	No deviations noted.
20	A risk assessment meeting of the management team is performed annually, in order to assess the risks identified and resolution of risks process	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key ControlUp stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were documented.	No deviations noted.

CC3.2 / COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
19	A risk assessment process is performed on, at least, an annual basis and documented within a dedicated file.	Inspected the risk assessment documentation and determined that a risk assessment process was performed on, at least, an annual basis and documented within a dedicated file.	No deviations noted.
20	A risk assessment meeting of the management team is performed annually, in order to assess the risks identified and resolution of risks process	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key ControlUp stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were documented.	No deviations noted.

CC3.3 / COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
19	A risk assessment process is performed on, at least, an annual basis and documented within a dedicated file.	Inspected the risk assessment documentation and determined that a risk assessment process was performed on, at least, an annual basis and documented within a dedicated file.	No deviations noted.
20	A risk assessment meeting of the management team is performed annually, in order to assess the risks identified and resolution of risks process	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key ControlUp stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were documented.	No deviations noted.

CC3.4 / COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Monthly management meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls and other strategic initiatives.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a monthly basis and that meeting minutes were retained.	No deviations noted.
66	A restore process is performed and documented on an annual basis.	Inspected the restoration test results and determined that the restore process was performed successfully and documented on an annual basis.	No deviations noted.
81	ControlUp has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of a disaster.	Inspected the Disaster Recovery Plan and determined that ControlUp had developed a Disaster Recovery Plan in order to continue to provide critical services in the event of a disaster.	No deviations noted.

Monitoring Activities

CC4.1 / COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
73	Service interruptions, maintenance and updates are communicated to customers through the company website	Inspected the ControlUp status page and determined that Service interruptions, maintenance and updates were communicated to customers through the company website	No deviations noted.
21	ControlUp uses a suite of monitoring tools in order to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules.	Inspected the ControlUp's monitoring dashboards and configuration and determined that ControlUp used a suite of monitoring tools to monitor its service and that alerts were sent to relevant stakeholders by an internal communication tool, based on pre-defined rules. Inspected the ControlUp's monitoring dashboards and configuration and determined that ControlUp used a suite of monitoring tools to monitor its service.	No deviations noted.
22	The production environment, including the servers and application, is monitored 24/7/365 by the NOC and Operations team. Key ControlUp staff is notified of events related to the security, availability or confidentiality of service to clients	Inspected the monitoring tool dashboards, rules and alerts and determined that the production environment, including the servers and application, was monitored 24/7/365 by the NOC and Operations team. Inspected a sample of notifications and determined that ControlUp staff was notified of events related to the security, availability or confidentiality of service to clients.	No deviations noted.
76	Actions performed on the production environment, including OS, DB and application are monitored and logged. This log is reviewed on a monthly basis by a dedicated personnel and alerts are triggered upon the identification of an anomaly.	Inspected the monitoring logs and determined that actions performed on the production and database environments were logged and reviewed. Inspected a sample of alerts and determined that alerts were triggered upon the identification of an anomaly.	No deviations noted.

CC4.2 / COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
73	Service interruptions, maintenance and updates are communicated to customers through the company website	Inspected the ControlUp status page and determined that Service interruptions, maintenance and updates were communicated to customers through the company website	No deviations noted.
21	ControlUp uses a suite of monitoring tools in order to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules.	Inspected the ControlUp's monitoring dashboards and configuration and determined that ControlUp used a suite of monitoring tools to monitor its service and that alerts were sent to relevant stakeholders by an internal communication tool, based on pre-defined rules. Inspected the ControlUp's monitoring dashboards and configuration and determined that ControlUp used a suite of monitoring tools to monitor its service.	No deviations noted.
22	The production environment, including the servers and application, is monitored 24/7/365 by the NOC and Operations team. Key ControlUp staff is notified of events related to the security, availability or confidentiality of service to clients	Inspected the monitoring tool dashboards, rules and alerts and determined that the production environment, including the servers and application, was monitored 24/7/365 by the NOC and Operations team. Inspected a sample of notifications and determined that ControlUp staff was notified of events related to the security, availability or confidentiality of service to clients.	No deviations noted.

Control Activities

CC5.1 / COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	There is a Company board that meets on at least a quarterly basis. The board meeting has a fixed agenda. Meeting minutes are retained.	Inspected a sample of meeting minutes and invitations and determined that board meetings were performed on at least a quarterly basis. The board meeting had a fixed agenda. Meeting minutes were retained	No deviations noted.
72	Security awareness training is performed on an annual basis. A link to the policies and procedures is provided at the end of the meeting.	Inspected the security awareness training documentation and determined that security awareness training was performed on an annual basis. A link to the policies and procedures was provided at the end of the meeting.	No deviations noted.
20	A risk assessment meeting of the management team is performed annually, in order to assess the risks identified and resolution of risks process	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key ControlUp stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were documented.	No deviations noted.

CC5.2 / COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	There is a Company board that meets on at least a quarterly basis. The board meeting has a fixed agenda. Meeting minutes are retained.	Inspected a sample of meeting minutes and invitations and determined that board meetings were performed on at least a quarterly basis. The board meeting had a fixed agenda. Meeting minutes were retained	No deviations noted.
3	Policies and procedures are documented, reviewed and approved on an annual basis and available to ControlUp's employees.	Inspected the policies and determined that policies were documented, reviewed and approved by management on an annual basis. Inspected the internal portal and determined that policies were available to employees.	No deviations noted.

CC5.3 / COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3	Policies and procedures are documented, reviewed and approved on an annual basis and available to ControlUp's employees.	Inspected the policies and determined that policies were documented, reviewed and approved by management on an annual basis. Inspected the internal portal and determined that policies were available to employees.	No deviations noted.
4	Monthly management meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls and other strategic initiatives.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a monthly basis and that meeting minutes were retained.	No deviations noted.
6	An organization chart is documented and approved by management that clearly defines management authorities and reporting hierarchy.	Inspected the company’s organization chart and determined that it was documented and approved by management. The organization chart clearly defined management authorities and reporting hierarchy.	No deviations noted.
71	A security policy is documented by ControlUp management, reviewed and approved on an annual basis by the COO and CO-Founder. The security policy is available to ControlUp's employees and reviewed annually within the shared folders.	Inspected the company security policy and determined that a security policy was documented by ControlUp management, reviewed and approved on an annual basis by the COO and CO-Founder. Inspected the company's shared folders and determined that the security policy was available to ControlUp's employees within the shared folders.	No deviations noted.

Logical and Physical Access Controls

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
23	The access to the production server is performed using a two-factor authentication method and through an email approval from the DevOps and is restricted to authorized personnel.	Inspected the list of users with access to the production servers and determined that it was performed by using a two factors authentication method and was restricted to authorized personnel. The approval was sent through email by the DevOps.	No deviations noted.
24	The access to the AWS management interface is performed using a two-factor authentication method.	Inspected the AWS access configurations and determined that the access to the AWS management interface was performed using a two factors authentication method.	No deviations noted.
25	The access to the AWS management interface is restricted to authorized personnel	Inspected the list of users with access to the AWS management servers and determined that access was restricted to authorized personnel.	No deviations noted.
26	The access to the servers is performed through RDP gateway.	Inspected the servers' access configuration and determined that access to the servers was performed through RDP gateway.	No deviations noted.
29	Access to the AWS resources is performed through a VPN or from the ControlUp offices.	Inspected the AWS access configuration and determined that access to the AWS resources was performed through a VPN or from the ControlUp offices' network.	No deviations noted.
30	Strong password configuration settings are enabled on the internal ControlUp domain using Group Policies. These settings include: (1) forced password change at defined intervals; (2) a minimum password length; (3) a limit on the number of unsuccessful attempts to enter a password before the user ID is suspended; and (4) password complexity requirements	Inspected the user group policies configuration and determined that strong password configuration settings were enabled on the internal ControlUp domain. These settings include: (1) forced password change at defined intervals; (2) a minimum password length; (3) a limit on the number of unsuccessful attempts to enter a password before the user ID was suspended; and (4) password complexity requirements.	No deviations noted.
34	The access to the offline storage, backup data, systems and media is restricted to authorized individuals.	Inspected the list of users with access permissions to the offline storage, backup data, systems and media and	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		determined that access was restricted to authorized individuals based.	
57	Developers do not have direct access to the production and database environment. The access is reviewed on a yearly basis. Specific developers can have access and log of actions are reviewed.	Inspected list of users with access to the production and their permissions and determined that developers did not have access to the production and database environment. Access was reviewed on a yearly basis. Specific developers can have access and log of actions were reviewed.	No deviations noted.
74	Access to sensitive permissions within the build tool is restricted authorized personnel.	Inspected the list of users with access to the build tool and determined that access to sensitive permissions within the build tool was restricted authorized personnel.	No deviations noted.
75	Single sign-on (SSO) is used for identity and access management (IAM) that enables users to securely authenticate with multiple applications and websites by logging with one set of credentials. The application relies on a trusted third party to verify the users.	Inspected the SSO configuration and determined that single sign-on (SSO) was used for identity and access management (IAM) that enabled users to securely authenticate with multiple applications and websites by logging with one set of credentials. The application relied on a trusted third party to verify the users.	No deviations noted.

CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
31	Terminated employees go through an off-boarding process and if they had an access to the production environment they have their permissions removed in a timely manner.	Inspected the offboarding checklist for a sample of terminated employees and determined that permissions were revoked in a timely manner.	No deviations noted.
32	New users accessing ControlUp system are granted access upon notification from the HR department. A detailed ticket is opened in the IT management ticketing system using a new hire template	Inspected the onboarding checklist for a sample of new employees and determined that new users accessing ControlUp system were granted access upon notification from the HR department. A detailed ticket was opened in the IT management ticketing system using a new hire template.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
35	Users, administrators and permissions within the production environment servers and database are reviewed and approved on a semi-annual basis by the VP and Director of Operation.	Inspected the full user access review document and determined that users, administrators and permissions within the production environment servers and database were reviewed and approved on a semi-annual basis by the VP and Director of Operation.	No deviations noted.

CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
31	Terminated employees go through an off-boarding process and if they had an access to the production environment they have their permissions removed in a timely manner.	Inspected the offboarding checklist for a sample of terminated employees and determined that permissions were revoked in a timely manner.	No deviations noted.
32	New users accessing ControlUp system are granted access upon notification from the HR department. A detailed ticket is opened in the IT management ticketing system using a new hire template	Inspected the onboarding checklist for a sample of new employees and determined that new users accessing ControlUp system were granted access upon notification from the HR department. A detailed ticket was opened in the IT management ticketing system using a new hire template.	No deviations noted.
35	Users, administrators and permissions within the production environment servers and database are reviewed and approved on a semi-annual basis by the VP and Director of Operation.	Inspected the full user access review document and determined that users, administrators and permissions within the production environment servers and database were reviewed and approved on a semi-annual basis by the VP and Director of Operation.	No deviations noted.

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
37	Physical access to ControlUp's office is restricted to authorized personnel using a personal identified card.	Inspected the physical access policy and performed a walkthrough of the ControlUp office and determined that physical access to ControlUp's office was restricted to authorized personnel using a personal identified card.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
38	Visitors to the ControlUp office are accompanied while on premises.	Inspected the physical access policy and performed a walkthrough of the ControlUp office and determined that visitors to the ControlUp office were accompanied while on premises.	No deviations noted.
82	ControlUp performs a review of the SOC 2 report of its datacenter on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at ControlUp to address the CUECs.	Inspected the review of the data center SOC 2 report performed by ControlUp.io and determined that the review was performed annually and included investigation of deviations and identifying and documenting the controls in place at ControlUp.io to address the CUECs.	No deviations noted.

CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
37	Physical access to ControlUp's office is restricted to authorized personnel using a personal identified card.	Inspected the physical access policy and performed a walkthrough of the ControlUp office and determined that physical access to ControlUp's office was restricted to authorized personnel using a personal identified card.	No deviations noted.
38	Visitors to the ControlUp office are accompanied while on premises.	Inspected the physical access policy and performed a walkthrough of the ControlUp office and determined that visitors to the ControlUp office were accompanied while on premises.	No deviations noted.
82	ControlUp performs a review of the SOC 2 report of its datacenter on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at ControlUp to address the CUECs.	Inspected the review of the data center SOC 2 report performed by ControlUp.io and determined that the review was performed annually and included investigation of deviations and identifying and documenting the controls in place at ControlUp.io to address the CUECs.	No deviations noted.

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
39	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.	Inspected the system architecture diagram and determined that access was protected through a combination of firewalls, VPNs, native operating system security, database management system security and application controls.	No deviations noted.
23	The access to the production server is performed using a two-factor authentication method and through an email approval from the DevOps and is restricted to authorized personnel.	Inspected the list of users with access to the production servers and determined that it was performed by using a two factors authentication method and was restricted to authorized personnel. The approval was sent through email by the DevOps.	No deviations noted.
26	The access to the servers is performed through RDP gateway.	Inspected the servers' access configuration and determined that access to the servers was performed through RDP gateway.	No deviations noted.
29	Access to the AWS resources is performed through a VPN or from the ControlUp offices.	Inspected the AWS access configuration and determined that access to the AWS resources was performed through a VPN or from the ControlUp offices' network.	No deviations noted.
30	Strong password configuration settings are enabled on the internal ControlUp domain using Group Policies. These settings include: (1) forced password change at defined intervals; (2) a minimum password length; (3) a limit on the number of unsuccessful attempts to enter a password before the user ID is suspended; and (4) password complexity requirements	Inspected the user group policies configuration and determined that strong password configuration settings were enabled on the internal ControlUp domain. These settings include: (1) forced password change at defined intervals; (2) a minimum password length; (3) a limit on the number of unsuccessful attempts to enter a password before the user ID was suspended; and (4) password complexity requirements.	No deviations noted.
34	The access to the offline storage, backup data, systems and media is restricted to authorized individuals.	Inspected the list of users with access permissions to the offline storage, backup data, systems and media and determined that access was restricted to authorized individuals based.	No deviations noted.
67	Clients’ sessions and interactions are encrypted using 256bit SSL V3/TLS HTTPS.	Inspected the platform encryption configuration and determined that clients’ sessions and interactions were encrypted using 256bit SSL V3/TLS.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
68	Database disks are encrypted using the AWS service using a KMS key. ControlUp end-point disks are encrypted as well.	Inspected the database encryption configuration and determined that database disks were encrypted using the Key Management Service operated by AWS.	No deviations noted.
69	Application server disks are encrypted when available and deemed necessary by ControlUp.	Inspected the application server disks configuration and determined that disks were encrypted when available and deemed necessary by ControlUp.	No deviations noted.
70	Confidentiality agreement is disclaimed as it relates to contracts with infrastructure third party providers in accordance with ControlUp confidentiality policy.	Inspected examples of signed business partners agreements and determined that the agreements contained a confidentiality clause.	No deviations noted.

CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
39	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.	Inspected the system architecture diagram and determined that access was protected through a combination of firewalls, VPNs, native operating system security, database management system security and application controls.	No deviations noted.
68	Database disks are encrypted using the AWS service using a KMS key. ControlUp end-point disks are encrypted as well.	Inspected the database encryption configuration and determined that database disks were encrypted using the Key Management Service operated by AWS.	No deviations noted.
69	Application server disks are encrypted when available and deemed necessary by ControlUp.	Inspected the application server disks configuration and determined that disks were encrypted when available and deemed necessary by ControlUp.	No deviations noted.

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
43	Penetration tests that help ensure the overall security status of the production platform and consistency with the confidentiality policy are performed on an annual basis.	Inspected the penetration test report and determined that it was performed on an annual basis. Inspected the penetration test report and determined that high issues were investigated and resolved.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
42	An antivirus is implemented within the ControlUp servers and within the employee's laptops.	Inspected the unified endpoint management tool configuration and dashboard and determined that an antivirus solution was installed on employees' laptops. Inspected a sample of antivirus reports and determined that the reports were sent to relevant stakeholders on a regular basis.	No deviations noted.

System Operations

CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
43	Penetration tests that help ensure the overall security status of the production platform and consistency with the confidentiality policy are performed on an annual basis.	Inspected the penetration test report and determined that it was performed on an annual basis. Inspected the penetration test report and determined that high issues were investigated and resolved.	No deviations noted.
42	An antivirus is implemented within the ControlUp servers and within the employee's laptops.	Inspected the unified endpoint management tool configuration and dashboard and determined that an antivirus solution was installed on employees' laptops. Inspected a sample of antivirus reports and determined that the reports were sent to relevant stakeholders on a regular basis.	No deviations noted.

CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
12	The SLA procedures are documented and available to customers on the company website. Tickets are classified and assigned to the relevant queue,	Inspected the Master Service Agreement that included the SLA and determined that the SLA procedures were documented and available to customers on the company website.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	handled by a dedicated support team. The issues are documented within the CRM tool.	Inspected the CRM tool and determined that tickets were classified and assigned to the relevant queue, handled by a dedicated support team. The issues were documented within the CRM tool	
15	ControlUp uses a third-party CRM application to manage, classify and ticket the client support-related issues. Tickets are classified by the level of urgency and assigned to the appropriate support tier for resolution.	Inspected a sample of client issues and determined that a CRM tool was used in order to manage client tickets. Tickets were prioritized according to the importance.	No deviations noted.
21	ControlUp uses a suite of monitoring tools in order to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules.	Inspected the ControlUp's monitoring dashboards and configuration and determined that ControlUp used a suite of monitoring tools to monitor its service and that alerts were sent to relevant stakeholders by an internal communication tool, based on pre-defined rules. Inspected the ControlUp's monitoring dashboards and configuration and determined that ControlUp used a suite of monitoring tools to monitor its service.	No deviations noted.
43	Penetration tests that help ensure the overall security status of the production platform and consistency with the confidentiality policy are performed on an annual basis.	Inspected the penetration test report and determined that it was performed on an annual basis. Inspected the penetration test report and determined that high issues were investigated and resolved.	No deviations noted.

CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
17	Support metrics (including Key Performance Indicators) are generated from the CRM application and sent to Company's stakeholders on a monthly basis.	Inspected a sample of KPI reports generated from the CRM application and determined that support metrics (including Key Performance Indicators) were generated from the CRM application and sent to Company's stakeholders on a monthly basis.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
21	ControlUp uses a suite of monitoring tools in order to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules.	Inspected the ControlUp's monitoring dashboards and configuration and determined that ControlUp used a suite of monitoring tools to monitor its service and that alerts were sent to relevant stakeholders by an internal communication tool, based on pre-defined rules. Inspected the ControlUp's monitoring dashboards and configuration and determined that ControlUp used a suite of monitoring tools to monitor its service.	No deviations noted.
44	Applicative anomalies are identified using pre-defined rules on a monitoring tool.	Inspected the monitoring tool configuration and a sample of alerts and determined that applicative anomalies were identified using pre-defined rules on a monitoring tool.	No deviations noted.
45	A vulnerability scan is performed on a quarterly basis using an automated external tool.	Inspected a sample of vulnerability test reports and determined that it was performed in the production environment at least on a quarterly basis, using an external tool, in order to detect potential security vulnerabilities.	No deviations noted.

CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
44	Applicative anomalies are identified using pre-defined rules on a monitoring tool.	Inspected the monitoring tool configuration and a sample of alerts and determined that applicative anomalies were identified using pre-defined rules on a monitoring tool.	No deviations noted.
45	A vulnerability scan is performed on a quarterly basis using an automated external tool.	Inspected a sample of vulnerability test reports and determined that it was performed in the production environment at least on a quarterly basis, using an external tool, in order to detect potential security vulnerabilities.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
77	The company has developed an incident management process in order to respond to Security Incidents and Personal Data Breaches in accordance with applicable laws and regulations.	Inspected the company incident management policy and determined that the company had developed an incident management process in order to respond to Security Incidents and Personal Data Breaches in accordance with applicable laws and regulations.	No deviations noted.
47	An incident application is available to ControlUp employees in order to report breaches in system security, availability, and confidentiality	Inspected the incident management application and determined that it was available to ControlUp employees in order to report breaches in system security, availability, and confidentiality.	No deviations noted.

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
73	Service interruptions, maintenance and updates are communicated to customers through the company website	Inspected the ControlUp status page and determined that Service interruptions, maintenance and updates were communicated to customers through the company website	No deviations noted.
44	Applicative anomalies are identified using pre-defined rules on a monitoring tool.	Inspected the monitoring tool configuration and a sample of alerts and determined that applicative anomalies were identified using pre-defined rules on a monitoring tool.	No deviations noted.
45	A vulnerability scan is performed on a quarterly basis using an automated external tool.	Inspected a sample of vulnerability test reports and determined that it was performed in the production environment at least on a quarterly basis, using an external tool, in order to detect potential security vulnerabilities	No deviations noted.
77	The company has developed an incident management process in order to respond to Security Incidents and Personal Data Breaches in accordance with applicable laws and regulations.	Inspected the company incident management policy and determined that the company had developed an incident management process in order to respond to Security Incidents and Personal Data Breaches in accordance with applicable laws and regulations.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
47	An incident application is available to ControlUp employees in order to report breaches in system security, availability, and confidentiality	Inspected the incident management application and determined that it was available to ControlUp employees in order to report breaches in system security, availability, and confidentiality.	No deviations noted.
66	A restore process is performed and documented on an annual basis.	Inspected the restoration test results and determined that the restore process was performed successfully and documented on an annual basis.	No deviations noted.

Change Management

CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
74	Access to sensitive permissions within the build tool is restricted authorized personnel.	Inspected the list of users with access to the build tool and determined that access to sensitive permissions within the build tool was restricted authorized personnel.	No deviations noted.
46	Operation requirements are being taken into consideration when a feature is approved to be developed. The VP operations are in charge of defining the operational needs.	Inspected documentation for a sample of features and determined that operation requirements were being taken into consideration when a feature was approved to be developed. The VP operations was in charge of defining the operational needs.	No deviations noted.
48	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.	For a sample of changes, inspected the change management tickets and determined that changes were documented, prioritized using tasks within the change management application. Tasks were prioritized according to their level of urgency and importance by the manager.	No deviations noted.
49	Weekly change management meetings are performed in order for the VP product to review and approve features.	Inspected a sample of weekly change management meeting invitations and determined that the meeting was performed in order for the VP product to review and approve features.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
62	A code review is performed and enforced within the source control application.	Inspected the pull requests for a sample of commits and determined that code review took place as part of the change management approval process. Inspected the source control tool configuration and determined that code review was mandatory to continue in the SDLC process.	No deviations noted.
51	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.	Inspected a sample of tasks created and determined that an acceptance test was performed by the QA team or feature owner from the Product team who approved it within the VSTS.	No deviations noted.
52	Permissions within the VSTS to move tasks from QA to close are restricted to authorized personnel.	Inspected the list of users with permissions within the VSTS to move tasks from QA to close and determined that it was restricted to authorized personnel.	No deviations noted.
53	Commits performed to the code within the source control are linked to a task within the change management application.	For a sample of changes, inspected the change management tickets and determined that commits performed to the code within the source control were linked to a task within the change management application.	No deviations noted.
55	Prior to moving a change to production, QA tests are documented and performed using pre-defined test scenarios.	Inspected the QA checks documentation and scenarios and determined that prior to moving a change to production, QA tests were documented and performed using pre-defined test scenarios.	No deviations noted.
56	Builds that went through QA testing successfully can be transferred to the production environment based on approval from the DevOps Manager.	For a sample of changes, inspected the tests that were performed for each change and the build configuration and determined that only builds that went through QA testing successfully could be transferred to the production environment based on approval from the DevOps Manager.	No deviations noted.
59	A monthly retrospective meeting is performed in order to review the SDLC process.	Inspected a sample of meeting minutes and determined that monthly retrospective meetings were performed in order to review the SDLC process.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
60	Database changes are performed using pre-approved scripts.	Inspected a sample of database changes and determined that database changes were performed using preapproved scripts.	No deviations noted.

Risk Mitigation

CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
20	A risk assessment meeting of the management team is performed annually, in order to assess the risks identified and resolution of risks process	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key ControlUp stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were documented.	No deviations noted.
78	Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the Company's objectives during response, mitigation, and recovery efforts.	Inspected the risk mitigation plan that included processing solutions to respond to, mitigate, and recover from security events that disrupt business operations and determined that the risk mitigation activities included the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures included monitoring processes and information and communications to meet the Company's objectives during the response, mitigation, and recovery efforts.	No deviations noted.

CC9.2: The entity assesses and manages risks associated with vendors and business partners.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
79	The Company assesses, on an annual basis, the risks that vendors and business partners (and those entities’ vendors and business partners) represent to the achievement of the Company's objectives.	Inspected the risk assessment and mapping documentation for vendors and business partners and determined that the Company assessed, on an annual basis, the risks that vendors and business partners (and those entities’ vendors and business partners) represent to the achievement of the Company's objectives.	No deviations noted.
70	Confidentiality agreement is disclaimed as it relates to contracts with infrastructure third party providers in accordance with ControlUp confidentiality policy.	Inspected examples of signed business partners agreements and determined that the agreements contained a confidentiality clause.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
82	ControlUp performs a review of the SOC 2 report of its datacenter on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at ControlUp to address the CUECs.	Inspected the review of the data center SOC 2 report performed by ControlUp.io and determined that the review was performed annually and included investigation of deviations and identifying and documenting the controls in place at ControlUp.io to address the CUECs.	No deviations noted.

Availability

A1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
21	ControlUp uses a suite of monitoring tools in order to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules.	Inspected the ControlUp's monitoring dashboards and configuration and determined that ControlUp used a suite of monitoring tools to monitor its service and that alerts were sent to relevant stakeholders by an internal communication tool, based on pre-defined rules. Inspected the ControlUp's monitoring dashboards and configuration and determined that ControlUp used a suite of monitoring tools to monitor its service.	No deviations noted.
63	Application backup is performed on a daily basis. Alerts are sent if the backup fails.	Inspected the database backup configuration and determined that the ControlUp application database was backed up on a daily basis. Alerts were sent if the fails.	No deviations noted.

A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
73	Service interruptions, maintenance and updates are communicated to customers through the company website	Inspected the ControlUp status page and determined that Service interruptions, maintenance and updates were communicated to customers through the company website	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
64	ControlUp’s application database and critical portions of the application file system are backed up incrementally on a daily basis.	Inspected the production database snapshot and determined that ControlUp’s application database and critical portions of the application file system were backed up incrementally on a daily basis.	No deviations noted.
80	ControlUp databases are replicated to multi availability zones	Inspected the configuration of ControlUp's databases and determined that they were replicated in several availability zones.	No deviations noted.

A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
66	A restore process is performed and documented on an annual basis.	Inspected the restoration test results and determined that the restore process was performed successfully and documented on an annual basis.	No deviations noted.
81	ControlUp has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of a disaster.	Inspected the Disaster Recovery Plan and determined that ControlUp had developed a Disaster Recovery Plan in order to continue to provide critical services in the event of a disaster.	No deviations noted.

Confidentiality

C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3	Policies and procedures are documented, reviewed and approved on an annual basis and available to ControlUp's employees.	Inspected the policies and determined that policies were documented, reviewed and approved by management on an annual basis. Inspected the internal portal and determined that policies were available to employees.	No deviations noted.
72	Security awareness training is performed on an annual basis. A link to the policies and procedures is provided at the end of the meeting.	Inspected the security awareness training documentation and determined that security awareness training was performed on an annual basis. A link to the policies and procedures was provided at the end of the meeting.	No deviations noted.
30	Strong password configuration settings are enabled on the internal ControlUp domain using Group Policies. These settings include: (1) forced password change at defined intervals; (2) a minimum password length; (3) a limit on the number of unsuccessful attempts to enter a password before the user ID is suspended; and (4) password complexity requirements	Inspected the user group policies configuration and determined that strong password configuration settings were enabled on the internal ControlUp domain. These settings include: (1) forced password change at defined intervals; (2) a minimum password length; (3) a limit on the number of unsuccessful attempts to enter a password before the user ID was suspended; and (4) password complexity requirements.	No deviations noted.
75	Single sign-on (SSO) is used for identity and access management (IAM) that enables users to securely authenticate with multiple applications and websites by logging with one set of credentials. The application relies on a trusted third party to verify the users.	Inspected the SSO configuration and determined that single sign-on (SSO) was used for identity and access management (IAM) that enabled users to securely authenticate with multiple applications and websites by logging with one set of credentials. The application relied on a trusted third party to verify the users.	No deviations noted.

C1.2 The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3	Policies and procedures are documented, reviewed, and approved on an annual basis and available to ControlUp's employees.	Inspected the company policies and procedures and determined that policies and procedures were documented, reviewed, and approved on an annual basis. Inspected the company policies and procedures and determined that policies and procedures were available to ControlUp's employees.	No deviations noted.
70	Confidentiality agreement is disclaimed as it relates to contracts with infrastructure third party providers in accordance with ControlUp confidentiality policy.	Inspected the contracts with third party providers and determined that a confidentiality agreement was disclaimed in accordance with ControlUp’s policy.	No deviations noted.

****