SOC 2 Type II Report

For the Period March 1, 2022 to February 28, 2023

REPORT ON CONTROLS PLACED IN OPERATION AT DOCONTROL INC.
RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY
WITH THE INDEPENDENT SERVICE AUDITOR'S REPORT
INCLUDING TESTS PERFORMED AND RESULTS THEREOF.

CONFIDENTIAL INFORMATION

Table of contents

Section I – DoControl Inc.'s Management Assertion

April 1, 2023

We have prepared the accompanying "Description of the DoControl Platform Relevant to Security, Availability and Confidentiality for the period March 1, 2022 to February 28, 2023" (Description) of DoControl Inc. (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 DoControl Platform (System) that may be useful when assessing the risks from interactions with the System throughout the period March 1, 2022 to February 28, 2023, 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).

DoControl Inc. uses Amazon Web Service to provide infrastructure management services. The Description includes only the controls of DoControl Inc. 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 DoControl Inc.'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 DoControl Inc.'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.

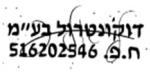
We confirm, to the best of our knowledge and belief, that:

a. The Description presents the System that was designed and implemented throughout the period March 1, 2022 to February 28, 2023 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 DoControl Inc.'s controls throughout the period March 1, 2022 to February 28, 2023.

c. The DoControl Inc. controls stated in the Description operated effectively throughout the period March 1, 2022 to February 28, 2023 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 DoControl Inc.'s controls throughout the period March 1, 2022 to February 28, 2023.

Liel Ran
CTO & Co-Founder



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

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

Section II - Independent service auditor's report

To the Management of DoControl Inc.

Scope

We have examined DoControl Inc.'s accompanying "Description of the DoControl Platform Relevant to Security, Availability and Confidentiality for the period March 1, 2022 to February 28, 2023" (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 March 1, 2022 to February 28, 2023 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).

DoControl Inc. uses Amazon Web Service ('AWS') (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 DoControl, to achieve DoControl's service commitments and system requirements based on the applicable trust services criteria. The description presents DoControl'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 AWS. Our examination did not extend to the services provided by AWS, and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period March 1, 2022 to February 28, 2023.

The Description also indicates that DoControl Inc.'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 DoControl'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.

DoControl's responsibilities

DoControl Inc. 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. DoControl Inc. has provided the accompanying assertion titled, "DoControl Inc. 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. DoControl Inc. 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 DoControl Platform system that was designed and implemented throughout the period March 1, 2022 to February 28, 2023 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 DoControl's controls throughout the period March 1, 2022 to February 28, 2023.

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 March 1, 2022 to February 28, 2023, if the subservice organization and user entity controls assumed in the design of DoControl's controls operated effectively throughout the period March 1, 2022 to February 28, 2023.

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 DoControl, user entities of DoControl's DoControl Platform during some or all of the period March 1, 2022 to February 28, 2023 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.

Kost Forer Gabbay and Kasierer

Kost Forer Gabbay and Kasierer
A member firm of Ernst & Young Global

April 1, 2023
Tel-Aviv, Israel

Section III - Description of the DoControl Platform relevant to Security, Availability and Confidentiality for the period March 1, 2022 to February 28, 2023

Company Overview and Background

DoControl is a US and Israeli based cyber security company that provides a SaaS platform focused on automated data access controls for SaaS and Cloud Applications. DoControl's solution is designed to improve security and operational efficiency with ease of use. DoControl's platform communicates with the Customer SaaS and Cloud platforms via the various platforms' APIs. Once the onboarding process is complete, a single point of view SaaS and Cloud Applications repository is created, allowing DoControl to provide its end-users and admins with end to end observability on all internal and external users within the SaaS and Cloud Applications, insights related to collaboration with external domains (e.g. outside of the customer organization), integrations with third-party applications and end-user behavior trends across SaaS and cloud applications. In addition, DoControl provides workflows and automation modules that help organizations achieve better control over their data, automatically revoke access based on a need to work basis and least privileges concepts.

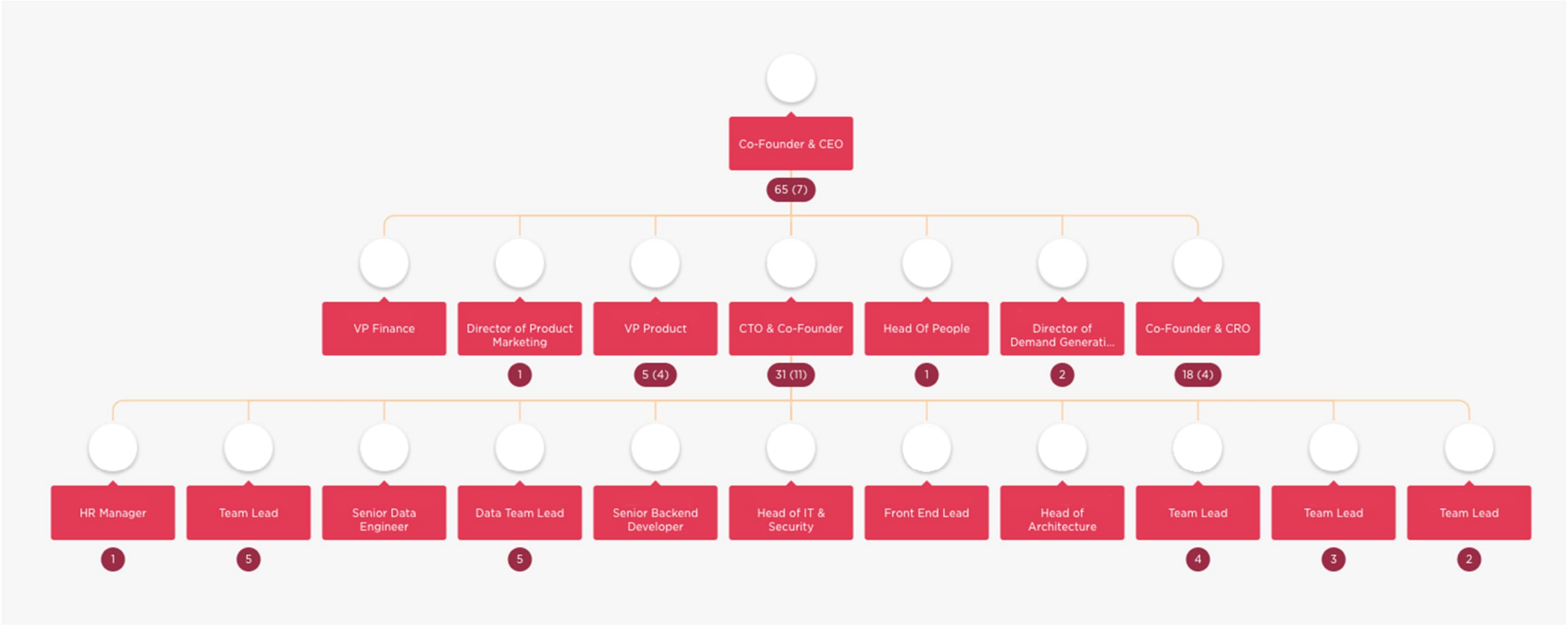
Purpose and Scope of the Report

The scope of this report is limited to the controls supporting the DoControl platform and not to the controls of the third-party service providers supporting DoControl's Production services (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, Controls, Tests and Results of Tests section of this report.

Organizational Structure

DoControl's organizational structure provides the framework within which its activities for achieving company-wide objectives are planned, executed, controlled and monitored. In addition, an organizational chart is documented and clearly defines the management's authorities and reporting hierarchy (3). The organizational structure is available internally for employees in a shared folder.



Below is a description of key DoControl departments:

- *Chief Revenue Officer (CRO):* Responsible for DoControl's revenue streams. Leveraging knowledge of the roles both sales and marketing play in driving growth, the CRO has the ultimate accountability in aligning all revenue-generating functions and building strategic partnerships. The CRO's cross-functional expertise ensures sales and marketing communications, shares information and collaborates in content creation so that all messaging fits their target customers.

- *Chief Technology Officer (CTO):* Responsible for DoControl's Technological efforts and activities including technological research, software development, engineering and technical operations of companywide assets including the production environment. The CTO is also responsible for IT and Security within the company.

- *Engineering:* Responsible for software development, maintenance and Research and Development (R&D) efforts. The engineering team reports to the CTO and is focused on designing and developing new features and capabilities of DoControl's product and services according to functional requirements and specifications defined by the Product function. In addition, R&D are responsible for maintaining and supporting the released products, including bug fixing and technical support for customer related issues in case where the issue is escalated to them. In addition to the software development, the engineering team is responsible for the overall management, operation and maintenance of DoControl's services availability, infrastructure and processing environment hosted on Amazon Web Services. This function is responsible for the deployment of new product versions, execution of configuration changes and maintenance activities to enable service reliability.

- *Product Management:* The primary goal of DoControl's Product Management function is to effectively manage the entire product lifecycle, from concept to general availability. The Product Management function focuses on translating market requirements into product requirements, assessing the feasibility of feature requests and prioritizing and defining the release scope. In addition, Product Management is responsible for defining the long-term product strategy and monitoring alignment with the overall company strategy and business objectives. The product management function is also responsible for gradually releasing feature flags for customers and communicating new features to customers.

- *Customer Success:* The Customer Success function is responsible to serve as the customer's voice at DoControl. This function is part of the Product Management team and provides ongoing account management, as well as technical and analysis support to ensure optimized usage of the DoControl services and customer satisfaction. DoControl provides customers with a direct, instant messaging-based communication channel for the Customer Success function.

- *Human Resources:* DoControl's Human Resources (HR) function is responsible for: (1) identifying and hiring competent personnel, (2) assisting executives in establishing human resource policies, (3) assisting employees with employment and benefits issues, (4) supporting the managers in their roles of overseeing employees and (5) supporting Company's compliance with employment laws and regulations.

Overview of Company's Internal Control

A company's internal control is a set of processes as determined by the Board of Directors, management and other leaders – 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 is a description of the five components of internal control for DoControl.

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. DoControl's executive management recognizes its responsibility for directing and controlling operations and for establishing, communicating and monitoring control policies and procedures.

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

Board of Directors: The DoControl Board of Directors meets quarterly and has a fixed agenda. The board establishes oversight responsibilities, applies relevant expertise and operates independently from management (1). The Board of Directors is composed of both independent directors and directors who are executive officers of the Company. The Board of Directors is actively engaged in the governance of the Company and its strategic direction.

Management: The DoControl management meets at least quarterly. The management meeting discusses operations, marketing and product issues (2). When applicable, these meetings address changes in significant laws and regulations that impact the Company or the industry.

Management Philosophy and Operating Style: DoControl's executives believe that DoControl's investors, shareholders, clients and employees are best served by an executive team that is highly involved in the day-to-day operations of the Company while giving employees the authority they need to properly serve their clients. Executives frequently visit offices and provide input they deem necessary and approve the actions taken. In addition, Executives are expected to be available to company managers to address significant issues during daily operations. Managers are encouraged to use similar strategies to enable clear communication and direction among their employees. Managers are encouraged to address developing issues and risks proactively to minimize the impact on the Company and its clients.

Integrity and Ethical Values: DoControl's values and behavioral standards have been established by management and approved by the Board of Directors. These values and standards are communicated to personnel through policy statements and a formal Code of Conduct which was adopted by the Board of Directors. The Code of Conduct is available to employees in the Company's shared folders. Compliance with the Code of Conduct and policy statements is enforced by management through a formal disciplinary process. Management demonstrates its commitment to the Code of Conduct by adhering to the policies and procedures of the Company.

Commitment to Competence: DoControl's HR policies and processes are 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 verify their ability to perform job assignments and (4) through the performance evaluation process, identify opportunities for growth and job performance improvement.

People and Human Resources: Controls are only as strong as the people that implement them. DoControl commits to employing competent individuals who possess the skills required to successfully implement the company's objectives. DoControl's products and services are created and delivered by the company's developers, product, marketing and customer success functions. Members are hired in line with hiring policies and procedures.

The HR function is responsible for the initial recruiting process and evaluation of job applicants together with the hiring managers including screening interviews. Further interviews with supervisors and management of the operating and functional teams are conducted in order to make final hiring decisions. HR is also responsible for performing reference checks on the candidates (in accordance with the DoControl background checks policy and subject to national law

restrictions). Job descriptions are documented and maintained within the DoControl collaboration environment. Candidates go through screening and appropriate reference checks (7). New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different DoControl policies and work procedures (8). Employee performance reviews are conducted at least on an annual basis for employees by their direct manager to increase communication, establish clear expectations, reinforce good performance, provide formal feedback to the employees and discuss employee needs related to training, tools and resources.

Risk Assessment

Risk identification: The process of identifying, assessing and managing risks is a critical component of DoControl's internal control system. The purpose of DoControl's risk assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives. Risk analysis includes the identification of key business processes in which potential exposures of some consequence exist. Exposures defined by DoControl, consider both internal and external influences that may harm the entity's ability to provide reliable services. It includes (1) identifying information assets, systems, virtual workloads, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets. It also includes the analysis of potential threats and vulnerabilities arising from critical vendors providing services, business partners, customers, and others with potential or actual access to DoControl's information systems. A comprehensive risk assessment that identifies and evaluates changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives is performed annually. As part of this process, threats to system security are identified, evaluated and the risk from these threats is formally assessed. The process is documented and approved by management (19).

Ongoing monitoring and risk assessment procedures are built into the normal recurring activities of DoControl and include regular management and supervisory activities. Identified risks are analyzed through a process that includes estimating the potential significance of the risk. The assessment includes how the risk should be managed and whether to accept, avoid, transfer or mitigate the risk. Managers of each team are regularly in touch with personnel and may question the accuracy of the information that differs significantly from their knowledge of operations. Key DoControl stakeholders evaluate risks and threats during a risk assessment meeting that takes place on an annual basis. Minutes of the meeting and action items are documented (20). DoControl 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 (21). DoControl has implemented a vendor management policy that includes a section on vendor termination. The policy is reviewed and approved annually (22).

Risk Mitigation: Once the severity and likelihood of a potential risk have 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. DoControl 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 aligned 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 DoControl's objectives during the response, mitigation, and recovery efforts.

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. DoControl's operating and functional units are required to implement

control activities that help achieve business objectives. DoControl has developed formal policies and procedures covering various operational matters to document the requirements for the performance of many control activities.

Security, Availability and Confidentiality policies are updated, reviewed and approved annually by the Chief Technology Officer (CTO). In addition, during the review, roles and responsibilities for developing and maintaining these policies are assigned. DoControl's Chief Security Officer is responsible and accountable for developing and maintaining policies around Security while the CTO is responsible and accountable for developing and maintaining policies around service availability. DoControl risk management approach is documented in its Risk Management policy, together with the actions taken to confirm that risks are constantly identified and handled. DoControl has developed a security incident response management policy. Root cause analysis is performed following security incidents (42).

Information and Communication

DoControl information is communicated and exchanged through meetings, emails, instant messaging, video and/or voice conferences. In addition, the company uses a cloud-based file sharing platform to share relevant documents and forms between employees. Access to the collaboration systems and platforms is restricted to authorized personnel using strong password configuration and multi factor authentication. Changes and updates to DoControl policies are communicated to DoControl employees through email or instant messaging updates by the company leadership team. Additionally, management subscribes to market research reports, news article clipping services, periodicals as well as general market trends and competitive risks and opportunities. The Marketing, Product and CTO functions within the Company distribute internal executive summaries of pertinent information within the Company to enable consistent understanding of new and developing issues. During the onboarding and kickoff process of a new customer, DoControl communicates the company support guidelines and support policy outlining the way to report service and availability issues. A "how to" guide is available to customers on how to use the product (14). There is an FAQ section available to customers on the company website (15). A description of the DoControl system and its boundaries is available to employees and customers on DoControl's website (4). Policies and procedures are documented, reviewed and approved on an annual basis by the management team and are available to DoControl's employees within the DoControl shared drive (5). Service interruptions and maintenance notifications are sent to customers (24).

Monitoring

Managers and supervisory personnel at DoControl are responsible for monitoring the quality and effectiveness of the various operations and internal controls as a routine part of their activities. DoControl has implemented multiple communication channels to monitor that processes function as they were designed, and potential issues are identified and resolved in a timely manner. DoControl managers are responsible for communicating relevant corporate information and job-related data to their direct employees.

Software Development Lifecycle (SDLC) Overview

Software development at DoControl is performed in a controlled manner, to help ensure applications are properly designed, tested, approved and aligned to the DoControl business objectives. Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by the management team within the Change Management application. Change Management tickets are prioritized and labeled (43). Code changes are reviewed along with the pull request performed by the team leader. The code review is documented on the version control system. Code review is mandatory in order to continue in the SDLC process and deploy a version to the production environment (45). Personnel responsible for the design, development, implementation and operation of systems affecting Security and Availability related issues have the qualifications and resources to fulfill their responsibilities.

New feature developments are initiated by the Product Management team while technical improvements and bug fixes are initiated by clients, R&D, Support and Customer Success. A dedicated platform that centralizes the Software Development Life Cycle is used to track, monitor and update the status throughout the process. New features are

communicated internally to employees via the internal communication platform (12). New features are communicated to customers periodically (13).

Development Methodology: DoControl software development method is based on the Scrum framework. The Scrum process is an agile process designed to manage and control development work based on (1) development teams (that integrate various stakeholders such as R&D and Product) working as a unit to reach its predefined goals, and (2) a day-to-day tracking and monitoring of the project progress, and (3) working in short development phases of 1-3 weeks, known as Sprints. The Scrum enables the development teams to improve communications and maximize cooperation. It also provides Product flexibility when deciding which requirements will be developed (beyond the current sprint) and therefore, it enables the product to quickly react to new requirements and needs coming from different stakeholders (e.g., customers, marketing, sales, etc.).

Each Sprint is managed by the Scrum Master, who is defined for each Scrum team. After each Sprint, a new release is ready to be deployed. Every new Sprint begins with Backlog Planning Session. DoControl performs a weekly R&D planning meeting with all the relevant stakeholders in order to plan the next release (48).

Before Sprint begins, Product, R&D team leaders and Business Development meet to plan the Sprint Backlog. Product leads this session and participants bring inputs on items to enter the coming sprint. Relevant items become backlog items that are considered for the next Sprint which is created in the application lifecycle management tool and a Product Owner is assigned to it.

The team prioritizes the items and decides which items are likely to enter the Sprint. After the meeting, R&D and QA team leaders break each of the Sprint backlog items into tasks (e.g., use-cases with functional requirements or test cases tasks), define resources and add work estimates for each. The Sprint backlog items may contain new requirements (e.g., new features or changes to existing features), as well as open bugs to be fixed.

On the first day of the Sprint, the Scrum team meets for a Sprint Planning Session. During the meeting, which is led by Product, the team reviews all sprint backlog items, definitions and estimates, implementing changes if required (based on clarifications and comments) and committing to the backlog items that will be included in the Sprint. Starting the 2nd day of the Sprint, the team meets daily for a short stand-up meeting, to review the progress, discuss open items or issues and update the relevant stakeholder on the Scrum status. In the meeting led by the Scrum Master, participants report on their progress since the previous meeting, what they are planning to complete until the next meeting and what current open issues require resolution (if any). Once R&D completes a backlog item task –the task is changed to status done. At the end of every Sprint, the team meets for a Sprint Review Session to evaluate planned work vs. actual work. In this session, each participant presents the items that were 'planned and done', 'planned and not done' or 'unplanned and done'.

Version control: The development environment enables multiple developers to collaborate on code development; changes to the code are tracked in a version control system. The version control system enables developers to check out complete copies of the project, make modifications and check in their work to the master copy. Changes in the change management tool are connected to the source control tool in order to link the request to the code change (44).

Software Testing and QA Process: Each development task inherently includes testing and QA processes. Once the R&D completes a development task, it will initiate testing cycles and change the task status to 'done'. The Product Owner reviews the results and the Production ready deliverable. The Engineering team will then deploy a new release with the relevant Product task implementation. The deployment is done gradually, using a "Feature Flag" that is enabled selectively to help enable safe testing of the developed feature. Once all backlog tasks are done (including testing tasks), the product will change the backlog item status to 'done', indicating that the backlog item is developed and tested. In

case of a bug, R&D will mark the R&D task as done. QA will then test the fix and label the bug with a 'verified' tag once successfully tested. The product will then confirm that the bug backlog item is done by changing its status to ‘done’.

Release testing: After the Sprint ends (in the following days), the Engineering team deploys the Sprint's final release on the Staging environment and QA tests the release as a unit, by performing Regression tests and 'Do no harm' tests on an internal customer-like environment. QA uses predefined test scenarios to perform these tests. Test results are sent to the relevant stakeholders. Bugs found by the QA team are opened in the development issue tracking tool. ProdOps deploy software builds to the Staging environments for testing.

Change Approval and production deployment: Only tested software builds that have successfully passed the automated checks and code review processes are qualified to be deployed to the production environment as part of a Continuous Integration and Deployment process (CI/CD). The Release Manager (ProdOps) captures the approvals as part of the Change Management procedure and deploys the release to production. The deployment of code to the production environment is performed by swapping between Staging and Production environments. Changes to the database environment used to support application changes are tracked and managed as a backlog item and those are included and described in the relevant change request forms. Changes performed to the application are communicated to DoControl clients by the customer success team, through release notes that are sent to them, once the changes are deployed and impacting the client.

DoControl uses a dedicated platform to manage its change items, their description and related tasks, testing requirements, current status and more. DoControl implements a build server to create versions. Versions are transferred to a QA environment where the QA performs and documents its testing activities and results. DoControl has multi-layer QA procedures: (1) unit tests (2) regression tests (3) end-to-end tests. Alerts are sent upon failover (51). Prior to the release deployment, the team confirms that the release change items are approved by QA (following successful testing), as well as other required approvals as described in the change management forms:

- Risks are evaluated.
- Rollback is available

Successful test status is required to continue in the SDLC process (49).

Infrastructure Change Management Process Overview

DoControl regularly makes changes within its production environment in response to evolving client and market needs. These changes include routine release deployments and maintenance activities. Change management procedures have been implemented to manage and maintain the production environment in an orderly and controlled manner in support of the business objectives of DoControl clients, protection of the availability and security of DoControl services and data and the minimization of potential risks to DoControl services that might occur as a result of such changes. Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved within the change management application.

The Engineering function is responsible to manage the production change process and its risks subject to the CTO’s approval. DoControl change management processes incorporate the following key components:

- Planning of changes
- Communication of change request items and plans to relevant stakeholders where applicable.
- Documentation of change request items, workflow and history in the ticketing system.
- Approval of change items prior to implementation.
- Production changes performed by authorized individuals only and automatically where possible.
- Execution of major changes within planned releases (sprints) as much as possible, in order to minimize potential risks to services and clients.

Prospective changes to the production environment are communicated and reviewed with the relevant stakeholders in a sync meeting and occur on a weekly basis. These meetings cover changes scheduled for the next deployment date and updates on deployments implemented since the last meeting.

DoControl uses internal forms and tickets to collect change items, related data, risks and approvals regarding production changes. A change request form is maintained for proposed releases to the production environment. In case of out-of-cycle releases, the team confirms that Product and Operations approvals were granted for the release. Scheduled releases are initiated by Product, which is also responsible to define their content.

Emergency Changes: An emergency change is a change deemed critical enough that it is implemented outside of the regular maintenance window and does not follow the routine approval process. In a case of an emergency change, authorized personnel make the change in order to maintain the level of service in the production environment. Emergency changes are documented, reviewed and approved according to the out of cycle change control process after the change has been implemented in production.

Segregation of Duties within the Change Management Process: DoControl implements segregation of duties throughout its change management process. Access to Production is performed using two-factor authentication and is restricted to authorized personnel (29). Access to the AWS Management platform, which allows implementing productions changes (such as infrastructure changes), as well as the permission to deploy new code to the production environment is restricted to authorized personnel using the need-to-work basis and least-privileges principles, thereby enabling DoControl to minimize the possibility of unauthorized changes. Permissions are granted to specific personnel according to an internal access control procedure. The permission to approve merge requests is restricted to authorized personnel (46). The permission to deploy is restricted to authorized personnel (47).

Security in the Development Life Cycle and Change Management Process

The DoControl security development lifecycle (SDLC) standard helps ensure the delivery of a highly secure platform. The following activities achieve this mission: DoControl maintains standards and documentation on secure development practices. Secure development guidance is provided to engineers as part of their team onboarding and to the entire engineering group on a periodical basis. This training provides engineers with the knowledge and capabilities to protect against the various types of potential attacks.

Security Reviews: DoControl products undergo security reviews, using both manual and automated processes, throughout each of the phases of the product lifecycle:

- Feature design – Identifying the security and compliance requirement the feature must adhere to.
- Development – Secure development environment and training are provided to each developer and code review is conducted on developed code
- Test – Security checks are conducted as part of manual and automated testing
- Release – A set of manual and automated scans are carried out against the application in a pre-production environment prior to release.

Logical Access and Physical Access

DoControl manages and delivers its services using a variety of systems and environments. 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 security, database management system security, application controls and intrusion detection monitoring software (28). Strict firewall rules, security groups or access lists are configured to protect network access and allow access to approved services. Logs are collected and monitored on a regular basis (38).

Access Control, Users and Permissions Management

DoControl ensures that users provisioned with access to systems and data managed by DoControl are granted access based on their job function and role using the principle of least privilege and need to know basis. DoControl employees are granted a limited set of default permissions to access company resources such as employee email, collaboration platforms and DoControl's internal systems. Additional permissions require a formal process that involves a request and approval from a manager as dictated by DoControl's security policies. An employee's authorization settings are used to control access to all resources, including data and systems. Access is periodically evaluated and revoked upon termination of the contract with DoControl. Users are identified through the use of a user ID, password and MFA. Strong password configuration settings, where applicable, are enabled including (1) forced password change at defined intervals, (2) a minimum password length, (3) a limit on the number of attempts to enter a password before the user ID is suspended, (4) password complexity and (5) Multi-Factor Authentication (27).

Access to customer data: Selected authorized DoControl staff are permitted to access the DoControl Production infrastructure only via a secure, highly restricted environment protected by multi-factor authentication and strict monitoring. Any access to customer data is audited, and alarms are configured to detect anomalous and potentially malicious activity pertaining to customer data.

Revoking Access Permissions

In order to prevent unauthorized access to data, user accounts within DoControl's various environments are disabled upon the termination of employment. Such permission revocation process is initiated once a termination notification is sent by the employee's direct manager or the HR manager, indicating the employee's expected last day to the relevant stakeholders such as the management, Finance, Operations and Engineering. Terminated employees complete a termination clearance process on their last day at DoControl. This process includes the revocation of access permissions to the DoControl systems. Terminated employees who had access to the production environment have their permissions removed in a timely manner (37). The CTO is responsible to confirm that the clearance process has been completed for the employee.

Recertification of Access Permissions

DoControl has implemented an access recertification process to help monitor that only authorized personnel have access to the systems, environments and databases. Permissions to the different environments (production, databases and applications) are reviewed, approved and documented by the DoControl management on a semi-annual basis (32). As part of the audit, a report listing the employees that have access to each production related environment or critical system is reviewed to confirm that it matches the definitions of employees whose job functions have evolved and who no longer require access to particular permissions, have their access disabled.

DoControl's Cloud Production Environment

DoControl's Production environment is based on multiple microservices and serverless functions hosted and operated within Amazon Web Services. Administrative access to the production environment is restricted to authorized personnel and is performed using MFA (30). AWS hosting facilities and infrastructure are compliant with a constantly growing set of standards and certifications including the SOC2 report that is reviewed by DoControl at least on an annual basis. For additional information about AWS security please refer to https://aws.amazon.com/security/.

Access to production servers is performed over VPN and Cloud credentials (33). Developers do not have modified access permission to the production environment. Specific developers can be granted access to specific projects or tasks, these accesses are logged and reviewed (31).

DoControl cloud workloads and service configuration processes are fully automated, to maintain the stability and reliability of the production environment. DoControl has a fully automated process for deploying new product versions.

Rollback is supported on all new deployments. The DoControl production environment is operated by engineers reporting to the CTO.

Datacenter

DoControl relies on AWS's Physical access methods, procedures and controls to prevent unauthorized access to data, assets and restricted areas. AWS complies, among others, with ISO 27001 and SOC2. DoControl performs a review of the SOC 2 report of its data center on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at DoControl to address the CUECs (36).

Offices

DoControl offices do not contain production servers or sensitive customer data. Physical access to the offices is restricted to authorized personnel with a pin code or a personal chip (34). Permissions to issue access tokens and grant access are restricted to the administrative manager and the authorized designees. Outside of working hours, the office doors are locked. During working hours, entrance is monitored and visitors (non-employees) are only allowed access accompanied by an employee. Visitors to the DoControl office are accompanied while on the premises (35). DoControl offices are also protected with CCTV. As part of the termination clearance process on their last day at DoControl, terminated employees or contractors return their access tokens and are disabled.

Collaboration with Customer Support & Customer communication

In case DoControl teams detect events related to the availability of service to clients, the Product owners are notified by instant messaging, email or phone. In addition, notifications and ongoing updates are sent to the product owner and key DoControl stakeholders. At times, clients may experience a local issue that prevents them from fully accessing or utilizing DoControl services. In such cases, the customer will inform DoControl, who in turn, escalates service availability issues to the Operations or Engineering team, to investigate the case. For the severity 1 event, the team creates a 'lessons learned' summary (postmortem) and distributes the event summary to key DoControl staff. Response time to customer issues is defined in the SLA agreement. The agreement is communicated to the customers as part of the contract (25).

Customer Success & Support

DoControl client support procedures are designed to handle and resolve issues and requests timely and efficiently. These include issues that are internally identified or submitted by clients. The DoControl Product and Customer Success team continuously monitor incoming requests and notifications from customers. Such incoming messages are documented within the Support ticketing and communication platform. Customer Success and Support is available during US work hours. Client issues are documented, resolved and closed by managing tickets in the ticketing platform. Tickets are classified to the level of urgency and importance. Customers can submit issues via a dedicated communication channel. Unresolved issues generate a ticket for further investigation and resolution based on priority (16). Support meetings are held at least twice a month in order to report major open issues to management and to gather feedback (17). A Product and Support meeting is held with the CEO, CTO, CRO and Head of Product to discuss and review ongoing service and product topics, customer requests and feedback. The topics and issues are reviewed, and development activities are prioritized based on internal criteria. Meeting summary is sent to meeting members. Support metrics are generated from the CRM application which includes Key Performance Indicators (KPI). The KPIs are sent to relevant stakeholders (18).

Customer Success Managers: Once a customer ticket is opened, the customer success manager contacts the customer for additional details if required and will begin the initial investigation and provide solutions. In the event that an issue cannot be resolved by the Support or CS team, it will be escalated to Operations/R&D for further investigation, while the customer success manager will remain the customer's focal point of contact. Once resolved, the customer success manager will update the customer via the ticketing system. Additionally, the customer success representative serves as the point of contact for all technical account management issues. The customer success managers will also receive direct emails from clients and may open customer tickets if required.

Ticketing and Management

DoControl opens a ticket when an issue is raised by a client. DoControl uses a third-party ticketing platform to manage, classify and track client support-related issues. Tickets are classified by their type and level of urgency. Issues escalated by the Customer Success management team to the development team are tracked and managed in the help desk ticketing tracking system. R&D related bugs are opened in the R&D issue tracking tool and managed there. Customer issues are also raised/discussed in the weekly internal customer meeting. Escalated alerts are reviewed by appropriate personnel and actions are performed in order to resolve issues in a timely manner.

Security Controls

In order to address security related risks, DoControl has implemented a robust security program, to protect the processes and technologies associated with its operations. This includes the establishment of a clear and documented security governance framework, adoption of an information security management system (ISMS), annual ISO27001 audit (in addition to the SOC2 audit), security processes around HR, Product, Infrastructure, Network, Cloud, Business Continuity, Incident Response and more. A security policy is documented, reviewed and approved by DoControl management on an annual basis. The security policy is available to DoControl employees within the DoControl shared drive (6). DoControl uses its own product for protecting its SaaS and Cloud application usage. In addition, antivirus software is installed on workstations, laptops, and servers supporting such software. DoControl uses a unified endpoint management tool in order to monitor its antivirus status (41). Security awareness training is held on an annual basis. Employees are required to pass a test at the end of the training (11). Personnel responsible for the design, development, implementation and operation of systems affecting security undergo training on an ad-hoc basis (10).

Penetration Testing

An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved (39). DoControl implements testing for security vulnerabilities on a regular basis using both built-in platform capabilities and external security assessment service providers. The penetration test is performed both against the platform as well as its underlying infrastructure. The penetration testing includes, among others, procedures to validate the controls that prevent customers, groups of individuals, or other entities from accessing information or resources they should not access. An executive summary is available for customer review upon request and is subject to NDA. High risks issues are followed up during the weekly management meetings and appropriate changes are acted upon in the review of the penetration test report. The CTO is responsible for executing the penetration tests and handling issues raised as part of the penetration test report.

Vulnerability Scan

Vulnerability assessments and tests are performed against the production environment at least on a weekly basis, using an external SaaS based tool, in order to detect potential security vulnerabilities on the internet facing attack surface. Vulnerability scans are performed on all the code using a dedicated tool in order to identify issues within the application (50). In addition, vulnerability scans are performed continuously in order to detect potential product issues. Tickets are created in order to track the issues found (40).

Availability Procedures

The DoControl production environment is fully managed by the DoControl Engineering team. DoControl has implemented the operations management controls described below to manage and execute production operations. DoControl production environment is located in several availability zones to maintain high availability standards (54).

Production Monitoring

DoControl uses a suite of monitoring tools to monitor its production environment. Alerts are sent to relevant stakeholders based on pre-defined rules. The notifications are reviewed and processed according to their level of urgency (23). DoControl production network encompasses numerous components, including serverless services, cloud computing,

workloads, databases and storage. In addition, security and monitoring tools are enabled within the production environment. To provide service availability to clients, the DoControl team uses different tools to monitor, identify and receive alerts on production issues. When events are detected, team members receive an email alert and may receive push notifications to their mobile devices. The team uses different tools to monitor production. Actions performed on the production environment, including OS, DB and application are monitored, logged and reviewed (26).

The team monitors a variety of system metrics in order to detect different production issues. e.g., metrics related to network, performance, number of API calls, transaction levels per customer, load on queues, sessions performance and much more. Issues detected are documented in the ticketing system and handled by priority.

Backup and Restoration

DoControl leverages multiple AWS availability zones to ensure the platform is highly reliable. The platform is designed for fault tolerance in a manner that ensures the DoControl service maintains availability in the event of multiple failure modes, including natural disasters and system failures.

Data Backup and restoration: DoControl performs daily, automated, backups of customer operational data and other critical data. The databases and production are automatically backed up on a daily basis. The data is retained for 35 days (52). All backups are encrypted in transit and at rest using industry standard encryption protocols. A restoration procedure exists and is exercised every six months.

Business Continuity Plan (BCP)

DoControl has established a business continuity plan (BCP) that enables the company to respond quickly and efficiently to unexpected or uncontrollable events that may result in a business interruption. DoControl has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of a disaster. The DRP is tested on annual basis. The results of the DRP are documented (53).

Confidentiality Procedures

Customer confidentiality is a key factor at DoControl. As such, DoControl has implemented security measures to ensure the confidentiality of its customer's sensitive personal information. Upon customer request at the end of an agreement, DoControl will dispose of customer confidential information (56). New vendors, business partners and subcontractors are required to sign an agreement containing a confidentiality clause (59). New employees are required to sign a standard employment agreement outlining confidentiality and intellectual property clauses (9).

DoControl's web tier and APIs are configured to force customer data to be encrypted in transit, using at least TLSv1.2 with the highest security setting available by AWS. Encryption between DoControl customers and the DoControl application is enabled using an authenticated SSL/TLS tunnel (57). Data at rest is encrypted (58). Customers' passwords/authentication tokens are encrypted (55).

Subservice Organization carved-out controls: 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, processing integrity availability and 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 and availability related policies.
- Provide that only authorized tested and documented changes are made to the system.
- Implement and maintain procedures exist and measures consistent with the risk assessment to protect the system against potential risks (for example, environmental risks, natural disasters, and routine operational errors and omissions) that might impair system processing integrity.

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 DoControl Inc., Kost Forer Gabbay & Kasierer (KFGK) considered the aspects of DoControl Inc.'s 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 DoControl Inc. The testing performed by KFGK and the results of the tests are the responsibility of the service auditor. Refer to the Trust Services criteria mapping section for the mapping of these controls to the Trust Services criteria.

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
7	Job descriptions are documented and maintained within the DoControl collaboration environment. Candidates go through screening and appropriate reference checks.	Inspected DoControl's website and determined that job descriptions were documented and maintained within the company website. Inspected the reference checks for a sample of new employees and determined that candidates went through screening and appropriate reference checks.	No deviations noted.
9	New employees are required to sign a standard employment agreement outlining confidentiality and 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.
59	New vendors, business partners and subcontractors are required to sign an agreement containing a confidentiality clause.	Inspected examples of signed business partners agreements and determined that the agreements contained a confidentiality clause.	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	The DoControl Board of Directors meets quarterly and has a fixed agenda. The board establishes oversight responsibilities, applies relevant expertise and operates independently from management.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that 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	The DoControl Board of Directors meets quarterly and has a fixed agenda. The board establishes	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	oversight responsibilities, applies relevant expertise and operates independently from management.		
2	The DoControl management meets at least quarterly. The management meeting discusses operations, marketing and product issues.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
3	An organizational chart is documented and clearly defines the management's authorities and reporting hierarchy.	Inspected DoControl's organizational chart and determined that the chart was documented and management authorities and reporting hierarchy were clearly defined.	No deviations noted.
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and are available to DoControl's employees within the DoControl shared drive.	Inspected the policies and determined that policies were documented, reviewed and approved by management on an annual basis. Inspected the DoControl shared drive and determined that policies were available to employees.	No deviations noted.
6	A security policy is documented, reviewed and approved by DoControl management on an annual basis. The security policy is available to DoControl employees within the DoControl shared drive.	Inspected DoControl's information security policy and determined that the policy was documented, reviewed and approved by management on an annual basis. Inspected the DoControl shared drive and determined that the policy was available to employees.	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 the DoControl collaboration environment. Candidates go through screening and appropriate reference checks.	Inspected DoControl's website and determined that job descriptions were documented and maintained within the company website.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the reference checks for a sample of new employees and determined that candidates went through screening and appropriate reference checks.	
8	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different DoControl policies and work procedures.	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 DoControl policies.	No deviations noted.
10	Personnel responsible for the design, development, implementation and operation of systems affecting security undergo training on an ad-hoc basis.	Inspected DoControl's training program and determined that training was performed on an ad-hoc basis by R&D personnel.	No deviations noted.
11	Security awareness training is held on an annual basis. Employees are required to pass a test at the end of the training.	Inspected security awareness training materials and the list of participants and determined that employees went through awareness training on an annual basis.	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
3	An organizational chart is documented and clearly defines the management's authorities and reporting hierarchy.	Inspected DoControl's organizational chart and determined that the chart was documented and management authorities and reporting hierarchy were clearly defined.	No deviations noted.
8	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different DoControl policies and work procedures.	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 DoControl policies.	No deviations noted.
9	New employees are required to sign a standard employment agreement outlining confidentiality and 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
10	Personnel responsible for the design, development, implementation and operation of systems affecting security undergo training on an ad-hoc basis.	Inspected DoControl'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
18	Support metrics are generated from the CRM application which includes Key Performance Indicators (KPI). The KPIs are sent to relevant stakeholders.	Inspected the CRM tool dashboards and determined that the support metrics were available. Inspected a sample of reports and determined that KPI reports were sent to relevant stakeholders.	No deviations noted.
20	Key DoControl stakeholders evaluate risks and threats during a risk assessment meeting that takes place on an annual basis. Minutes of the meeting and action items are documented.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key DoControl 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
4	A description of the DoControl system and its boundaries is available to employees and customers on DoControl's website.	Inspected DoControl's website and determined that a description of the DoControl system and its boundaries were documented and available to employees and to customers.	No deviations noted.
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and are available to DoControl's employees within the DoControl shared drive.	Inspected the policies and determined that policies were documented, reviewed and approved by management on an annual basis.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the DoControl shared drive and determined that policies were available to employees.	
6	A security policy is documented, reviewed and approved by DoControl management on an annual basis. The security policy is available to DoControl employees within the DoControl shared drive.	Inspected DoControl's information security policy and determined that the policy was documented, reviewed and approved by management on an annual basis. Inspected the DoControl shared drive and determined that the policy was available to employees.	No deviations noted.
8	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different DoControl policies and work procedures.	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 DoControl policies.	No deviations noted.
11	Security awareness training is held on an annual basis. Employees are required to pass a test at the end of the training.	Inspected security awareness training materials and the list of participants and determined that employees went through awareness training on an annual basis.	No deviations noted.
12	New features are communicated internally to employees via the internal communication platform.	Inspected a sample of release notes and determined that new features were communicated to employees via the internal communication platform.	No deviations noted.
16	Customers can submit issues via a dedicated communication channel. Unresolved issues generate a ticket for further investigation and resolution based on priority.	Inspected a sample of support tickets and determined that unresolved issues were investigated and resolved based on priority.	No deviations noted.
18	Support metrics are generated from the CRM application which includes Key Performance Indicators (KPI). The KPIs are sent to relevant stakeholders.	Inspected the CRM tool dashboards and determined that the support metrics were available. Inspected a sample of reports and determined that KPI reports were sent to relevant stakeholders.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
25	Response time to customer issues is defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.	Inspected the internal company's SLA agreement and determined that response time to customer's issues was defined in the company's SLA.	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	A description of the DoControl system and its boundaries is available to employees and customers on DoControl's website.	Inspected DoControl's website and determined that a description of the DoControl system and its boundaries were documented and available to employees and to customers.	No deviations noted.
13	New features are communicated to customers periodically.	Inspected a sample of release notes and determined that new features were communicated to customers through emails, the website or directly through the account manager.	No deviations noted.
14	A "how to" guide is available to customers on how to use the product.	Inspected the company website and determined that a knowledge base was available to guide customers on how to use the product.	No deviations noted.
15	There is an FAQ section available to customers on the company website.	Inspected the FAQ section within the company's website and determined that a knowledge base was available to guide customers on how to use the product.	No deviations noted.
16	Customers can submit issues via a dedicated communication channel. Unresolved issues generate a ticket for further investigation and resolution based on priority.	Inspected a sample of support tickets and determined that unresolved issues were investigated and resolved based on priority.	No deviations noted.
24	Service interruptions and maintenance notifications are sent to customers.	Inspected DoControl's system uptime report throughout the audit period and determined that there were no significant downtimes during the audit period.	No deviations noted.
25	Response time to customer issues is defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.	Inspected the internal company's SLA agreement and determined that response time to customer's issues was defined in the company's SLA.	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 comprehensive risk assessment that identifies and evaluates changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives is performed annually. As part of this process, threats to system security are identified, evaluated and the risk from these threats is formally assessed. The process is documented and approved by management.	Inspected the risk assessment documentation and determined that it was performed and documented annually.	No deviations noted.
20	Key DoControl stakeholders evaluate risks and threats during a risk assessment meeting that takes place on an annual basis. Minutes of the meeting and action items are documented.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key DoControl 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
1	The DoControl Board of Directors meets quarterly and has a fixed agenda. The board establishes oversight responsibilities, applies relevant expertise and operates independently from management.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The DoControl management meets at least quarterly. The management meeting discusses operations, marketing and product issues.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a quarterly basis and that meeting minutes were retained.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
19	A comprehensive risk assessment that identifies and evaluates changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives is performed annually. As part of this process, threats to system security are identified, evaluated and the risk from these threats is formally assessed. The process is documented and approved by management.	Inspected the risk assessment documentation and determined that it was performed and documented annually.	No deviations noted.
20	Key DoControl stakeholders evaluate risks and threats during a risk assessment meeting that takes place on an annual basis. Minutes of the meeting and action items are documented.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key DoControl stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were documented.	No deviations noted.
40	Vulnerability scans are performed continuously in order to detect potential product issues. Tickets are created in order to track the issues found.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously to detect potential product issues. Inspected an example of a vulnerability ticket and determined that vulnerabilities were tracked until resolution.	No deviations noted.
50	Vulnerability scans are performed on all the code using a dedicated tool in order to identify issues within the application.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously on source code.	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
1	The DoControl Board of Directors meets quarterly and has a fixed agenda. The board establishes	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	oversight responsibilities, applies relevant expertise and operates independently from management.		
2	The DoControl management meets at least quarterly. The management meeting discusses operations, marketing and product issues.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
19	A comprehensive risk assessment that identifies and evaluates changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives is performed annually. As part of this process, threats to system security are identified, evaluated and the risk from these threats is formally assessed. The process is documented and approved by management.	Inspected the risk assessment documentation and determined that it was performed and documented annually.	No deviations noted.
20	Key DoControl stakeholders evaluate risks and threats during a risk assessment meeting that takes place on an annual basis. Minutes of the meeting and action items are documented.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key DoControl 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
1	The DoControl Board of Directors meets quarterly and has a fixed agenda. The board establishes oversight responsibilities, applies relevant expertise and operates independently from management.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The DoControl management meets at least quarterly. The management meeting discusses operations, marketing and product issues.	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
		met on a quarterly basis and that meeting minutes were retained.	
39	An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved.	Inspected the penetration test report and determined that it was performed on an annual basis. Inspected the penetration test report and determined that critical and high issues were investigated and resolved.	No deviations noted.
40	Vulnerability scans are performed continuously in order to detect potential product issues. Tickets are created in order to track the issues found.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously to detect potential product issues. Inspected an example of a vulnerability ticket and determined that vulnerabilities were tracked until resolution.	No deviations noted.
50	Vulnerability scans are performed on all the code using a dedicated tool in order to identify issues within the application.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously on source code.	No deviations noted.
53	DoControl has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of a disaster. The DRP is tested on annual basis. The results of the DRP are documented.	Inspected the Disaster Recovery Plan and determined that the policy was reviewed and approved on an annual basis. Inspected the Disaster Recovery test and determined that the DRP was tested on an annual basis.	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
21	DoControl 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 vendor assessment and determined that vendors were assessed annually for the risk they may represent to the achievement of the company's objectives.	No deviations noted.
23	DoControl uses a suite of monitoring tools to monitor its production environment. Alerts are sent to relevant stakeholders based on pre-defined rules. The notifications are reviewed and processed according to their level of urgency.	Inspected DoControl's monitoring dashboards and configuration and determined that DoControl 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.	No deviations noted.
26	Actions performed on the production environment, including OS, DB and application are monitored, logged and reviewed.	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
1	The DoControl Board of Directors meets quarterly and has a fixed agenda. The board establishes oversight responsibilities, applies relevant expertise and operates independently from management.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The DoControl management meets at least quarterly. The management meeting discusses operations, marketing and product issues.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a quarterly basis and that meeting minutes were retained.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
17	Support meetings are held at least twice a month in order to report major open issues to management and to gather feedback.	Inspected a sample of support meeting minutes and invitations and determined that support meetings were performed on a bi-weekly basis to review customer issues and requests.	No deviations noted.
23	DoControl uses a suite of monitoring tools to monitor its production environment. Alerts are sent to relevant stakeholders based on pre-defined rules. The notifications are reviewed and processed according to their level of urgency.	Inspected DoControl's monitoring dashboards and configuration and determined that DoControl 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.	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
20	Key DoControl stakeholders evaluate risks and threats during a risk assessment meeting that takes place on an annual basis. Minutes of the meeting and action items are documented.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key DoControl 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
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and are available to DoControl's employees within the DoControl shared drive.	Inspected the policies and determined that policies were documented, reviewed and approved by management on an annual basis. Inspected the DoControl shared drive and determined that policies were available to employees.	No deviations noted.
11	Security awareness training is held on an annual basis. Employees are required to pass a test at the end of the training.	Inspected security awareness training materials and the list of participants and determined that employees went through awareness training on an annual basis.	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	An organizational chart is documented and clearly defines the management's authorities and reporting hierarchy.	Inspected DoControl's organizational chart and determined that the chart was documented and management authorities and reporting hierarchy were clearly defined.	No deviations noted.
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and are available to DoControl's employees within the DoControl shared drive.	Inspected the policies and determined that policies were documented, reviewed and approved by management on an annual basis. Inspected the DoControl shared drive and determined that policies were available to employees.	No deviations noted.
6	A security policy is documented, reviewed and approved by DoControl management on an annual basis. The security policy is available to DoControl employees within the DoControl shared drive.	Inspected DoControl's information security policy and determined that the policy was documented, reviewed and approved by management on an annual basis. Inspected the DoControl shared drive and determined that the policy was available to employees.	No deviations noted.
16	Customers can submit issues via a dedicated communication channel. Unresolved issues generate a ticket for further investigation and resolution based on priority.	Inspected a sample of support tickets and determined that unresolved issues were investigated and resolved based on priority.	No deviations noted.
22	DoControl has implemented a vendor management policy that includes a section on vendor termination. The policy is reviewed and approved annually.	Inspected the vendor management policy and determined that DoControl detailed the vendor termination process and that the policy was reviewed and approved annually.	No deviations noted.
25	Response time to customer issues is defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.	Inspected the internal company's SLA agreement and determined that response time to customer’s issues was defined in the company's SLA.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
53	DoControl has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of a disaster. The DRP is tested on annual basis. The results of the DRP are documented.	Inspected the Disaster Recovery Plan and determined that the policy was reviewed and approved on an annual basis. Inspected the Disaster Recovery test and determined that the DRP was tested on an annual basis.	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
27	Users are identified through the use of a user ID, password and MFA. Strong password configuration settings, where applicable, are enabled including (1) forced password change at defined intervals, (2) a minimum password length, (3) a limit on the number of attempts to enter a password before the user ID is suspended, (4) password complexity and (5) Multi-Factor Authentication.	Inspected the Okta Single Sign-On password configuration settings and determined that strong password configuration settings, where applicable, were enabled on Okta and native tools including (1) forced password change at defined intervals, (2) a minimum password length, (3) a limit on the number of attempts to enter a password before the user ID was suspended, and (4) password complexity (5) Multi-Factor Authentication.	No deviations noted.
29	Access to production is performed using two-factor authentication and is restricted to authorized personnel.	Inspected the list of users with access to the production and determined it was restricted to authorized personnel. Inspected the production access configuration and determined that two-factor authentication was enabled.	No deviations noted.
30	Administrative access to the production environment is restricted to authorized personnel and is performed using MFA.	Inspected the list of users with access to the production environment and determined that administrative access was restricted to authorized personnel.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the production environment access configuration and determined that MFA was enabled.	
31	Developers do not have modified access permission to the production environment. Specific developers can be granted access to specific projects or tasks, these accesses are logged and reviewed.	Inspected the list of users with access permissions to the production environment and determined that developers did not have access to the production. Inspected the log configuration and determined that accesses were logged and reviewed.	No deviations noted.
33	Access to production servers is performed over VPN and Cloud credentials.	Inspected the list of users with access to the production server by VPN connection and Cloud credentials and determined it was restricted to authorized personnel.	No deviations noted.
38	Strict firewall rules, security groups or access lists are configured to protect network access and allow access to approved services. Logs are collected and monitored on a regular basis.	Inspected the configuration settings and determined that rules were configured to protect network access and allow access to approved services. Inspected the list of users with access to the firewall management tool and determined that access was restricted to authorized personnel.	No deviations noted.
46	The permission to approve merge requests is restricted to authorized personnel.	Inspected the list of users with permission to approve merge requests and determined that it was restricted to authorized personnel.	No deviations noted.
47	The permission to deploy is restricted to authorized personnel.	Inspected the list of users with permission to deploy and determined that it was restricted to authorized personnel.	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
32	Permissions to the different environments (production, databases and applications) are	Inspected the user access review documentation and determined that accesses and permissions for the	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	reviewed, approved and documented by the DoControl management on a semi-annual basis.	different environments were reviewed and approved by the management on a semi-annual basis.	
37	Terminated employees who had access to the production environment 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 and assets were returned.	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
32	Permissions to the different environments (production, databases and applications) are reviewed, approved and documented by the DoControl management on a semi-annual basis.	Inspected the user access review documentation and determined that accesses and permissions for the different environments were reviewed and approved by the management on a semi-annual basis.	No deviations noted.
37	Terminated employees who had access to the production environment 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 and assets were returned.	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
34	Physical access to the offices is restricted to authorized personnel with a pin code or a personal chip.	Inspected the physical access policy and determined that physical access was restricted to authorized personnel using a pin code or a personal chip.	No deviations noted.
35	Visitors to the DoControl office are accompanied while on the premises.	Inspected the physical access policy and determined that visitors were accompanies while on premises.	No deviations noted.
36	DoControl performs a review of the SOC 2 report of its data center on an annual basis. Deviations are investigated. The review includes identifying and	Inspected the review of the data center SOC 2 report performed by DoControl and determined that the review was performed annually and included	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	documenting the controls in place at DoControl to address the CUECs.	investigation of deviations and identifying and documenting the controls in place at DoControl to address the CUECs.	

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
36	DoControl performs a review of the SOC 2 report of its data center on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at DoControl to address the CUECs.	Inspected the review of the data center SOC 2 report performed by DoControl and determined that the review was performed annually and included investigation of deviations and identifying and documenting the controls in place at DoControl 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
28	Access to system resources is protected through a combination of firewalls, VPNs, native operating system security, 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 application controls and intrusion detection monitoring software.	No deviations noted.
57	Encryption between DoControl customers and the DoControl application is enabled using an authenticated SSL/TLS tunnel.	Inspected the encryption configuration and determined that the encryption between DoControl customers and the DoControl application was enabled using an authenticated SSL tunnel.	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
28	Access to system resources is protected through a combination of firewalls, VPNs, native operating system security, 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 application controls and intrusion detection monitoring software.	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
39	An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved.	Inspected the penetration test report and determined that it was performed on an annual basis. Inspected the penetration test report and determined that critical and high issues were investigated and resolved.	No deviations noted.
40	Vulnerability scans are performed continuously in order to detect potential product issues. Tickets are created in order to track the issues found.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously to detect potential product issues. Inspected an example of a vulnerability ticket and determined that vulnerabilities were tracked until resolution.	No deviations noted.
41	Antivirus software is installed on workstations, laptops, and servers supporting such software. DoControl uses a unified endpoint management tool in order to monitor its antivirus status.	Inspected a sample of employees' laptops and dashboards and determined that an antivirus solution was installed on employees' laptops.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
50	Vulnerability scans are performed on all the code using a dedicated tool in order to identify issues within the application.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously on source code.	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
39	An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved.	Inspected the penetration test report and determined that it was performed on an annual basis. Inspected the penetration test report and determined that critical and high issues were investigated and resolved.	No deviations noted.
40	Vulnerability scans are performed continuously in order to detect potential product issues. Tickets are created in order to track the issues found.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously to detect potential product issues. Inspected an example of a vulnerability ticket and determined that vulnerabilities were tracked until resolution.	No deviations noted.
41	Antivirus software is installed on workstations, laptops, and servers supporting such software. DoControl uses a unified endpoint management tool in order to monitor its antivirus status.	Inspected a sample of employees' laptops and dashboards and determined that an antivirus solution was installed on employees' laptops.	No deviations noted.
50	Vulnerability scans are performed on all the code using a dedicated tool in order to identify issues within the application.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously on source code.	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
16	Customers can submit issues via a dedicated communication channel. Unresolved issues generate a ticket for further investigation and resolution based on priority.	Inspected a sample of support tickets and determined that unresolved issues were investigated and resolved based on priority.	No deviations noted.
23	DoControl uses a suite of monitoring tools to monitor its production environment. Alerts are sent to relevant stakeholders based on pre-defined rules. The notifications are reviewed and processed according to their level of urgency.	Inspected DoControl’s monitoring dashboards and configuration and determined that DoControl 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.	No deviations noted.
25	Response time to customer issues is defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.	Inspected the internal company's SLA agreement and determined that response time to customer’s issues was defined in the company's SLA.	No deviations noted.
39	An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved.	Inspected the penetration test report and determined that it was performed on an annual basis. Inspected the penetration test report and determined that critical and 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
23	DoControl uses a suite of monitoring tools to monitor its production environment. Alerts are sent to relevant stakeholders based on pre-defined rules. The notifications are reviewed and processed according to their level of urgency.	Inspected DoControl’s monitoring dashboards and configuration and determined that DoControl 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.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
40	Vulnerability scans are performed continuously in order to detect potential product issues. Tickets are created in order to track the issues found.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously to detect potential product issues. Inspected an example of a vulnerability ticket and determined that vulnerabilities were tracked until resolution.	No deviations noted.
42	DoControl has developed a security incident response management policy. Root cause analysis is performed following security incidents.	Inspected the incident management policy and determined it included guidelines on how to perform a root cause analysis. During the audit period, no security events occurred.	No deviations noted.
50	Vulnerability scans are performed on all the code using a dedicated tool in order to identify issues within the application.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously on source code.	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
40	Vulnerability scans are performed continuously in order to detect potential product issues. Tickets are created in order to track the issues found.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously to detect potential product issues. Inspected an example of a vulnerability ticket and determined that vulnerabilities were tracked until resolution.	No deviations noted.
42	DoControl has developed a security incident response management policy. Root cause analysis is performed following security incidents.	Inspected the incident management policy and determined it included guidelines on how to perform a root cause analysis. During the audit period, no security events occurred.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
50	Vulnerability scans are performed on all the code using a dedicated tool in order to identify issues within the application.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously on source code.	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
24	Service interruptions and maintenance notifications are sent to customers.	Inspected DoControl's system uptime report throughout the audit period and determined that there were no significant downtimes during the audit period.	No deviations noted.
40	Vulnerability scans are performed continuously in order to detect potential product issues. Tickets are created in order to track the issues found.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously to detect potential product issues. Inspected an example of a vulnerability ticket and determined that vulnerabilities were tracked until resolution.	No deviations noted.
42	DoControl has developed a security incident response management policy. Root cause analysis is performed following security incidents.	Inspected the incident management policy and determined it included guidelines on how to perform a root cause analysis. During the audit period, no security events occurred.	No deviations noted.
50	Vulnerability scans are performed on all the code using a dedicated tool in order to identify issues within the application.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously on source code.	No deviations noted.
53	DoControl has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of a disaster. The DRP is tested on annual basis. The results of the DRP are documented.	Inspected the Disaster Recovery Plan and determined that the policy was reviewed and approved on an annual basis. Inspected the Disaster Recovery test and determined that the DRP was tested 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
43	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by the management team within the Change Management application. Change Management tickets are prioritized and labeled.	Inspected a sample of change management tickets and determined that changes were documented, prioritized and labeled based on development phase and urgency. Inspected the change management tickets for a sample of pull requests and determined that tickets contained a documented description of the required change.	No deviations noted.
44	Changes in the change management tool are connected to the source control tool in order to link the request to the code change.	Inspected a sample of change management tickets and determined they were linked to the actual code in the version control tool.	No deviations noted.
45	Code changes are reviewed along with the pull request performed by the team leader. The code review is documented on the version control system. Code review is mandatory in order to continue in the SDLC process and deploy a version to the production environment.	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.
48	DoControl performs a weekly R&D planning meeting with all the relevant stakeholders in order to plan the next release.	Inspected a sample of R&D planning meeting invitations and determined that meetings took place every week with all the relevant stakeholders in order to plan the next release.	No deviations noted.
49	Successful test status is required to continue in the SDLC process.	Inspected the source control tool's configuration and determined that a successful test status was mandatory in order to continue with the SDLC process.	No deviations noted.
51	DoControl has multi-layer QA procedures: (1) unit tests (2) regression tests (3) end-to-end tests. Alerts are sent upon failover.	Inspected the pull requests for a sample of commits and determined that changes went through automation testing.	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
9	New employees are required to sign a standard employment agreement outlining confidentiality and 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.
20	Key DoControl stakeholders evaluate risks and threats during a risk assessment meeting that takes place on an annual basis. Minutes of the meeting and action items are documented.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key DoControl stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were documented.	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
2	The DoControl management meets at least quarterly. The management meeting discusses operations, marketing and product issues.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
21	DoControl 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 vendor assessment and determined that vendors were assessed annually for the risk they may represent to the achievement of the company's objectives.	No deviations noted.
22	DoControl has implemented a vendor management policy that includes a section on vendor termination. The policy is reviewed and approved annually.	Inspected the vendor management policy and determined that DoControl detailed the vendor termination process and that the policy was reviewed and approved annually.	No deviations noted.
34	Physical access to the offices is restricted to authorized personnel with a pin code or a personal chip.	Inspected the physical access policy and determined that physical access was restricted to authorized personnel using a pin code or a personal chip.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
35	Visitors to the DoControl office are accompanied while on the premises.	Inspected the physical access policy and determined that visitors were accompanies while on premises.	No deviations noted.
36	DoControl performs a review of the SOC 2 report of its data center on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at DoControl to address the CUECs.	Inspected the review of the data center SOC 2 report performed by DoControl and determined that the review was performed annually and included investigation of deviations and identifying and documenting the controls in place at DoControl to address the CUECs.	No deviations noted.
59	New vendors, business partners and subcontractors are required to sign an agreement containing a confidentiality clause.	Inspected examples of signed business partners agreements and determined that the agreements contained a confidentiality clause.	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
23	DoControl uses a suite of monitoring tools to monitor its production environment. Alerts are sent to relevant stakeholders based on pre-defined rules. The notifications are reviewed and processed according to their level of urgency.	Inspected DoControl's monitoring dashboards and configuration and determined that DoControl 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.	No deviations noted.
54	DoControl production environment is located in several availability zones to maintain high availability standards.	Inspected a configuration of the DoControl production environment and determined that it was replicated to several availability zones to maintain high availability standards.	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
24	Service interruptions and maintenance notifications are sent to customers.	Inspected DoControl's system uptime report throughout the audit period and determined that there were no significant downtimes during the audit period.	No deviations noted.
52	The databases and production are automatically backed up on a daily basis. The data is retained for 35 days.	Inspected the database backup configuration and determined that the DoControl application database was backed up on a daily basis and data was retained for 35 days.	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
53	DoControl has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of a disaster. The DRP is tested on annual basis. The results of the DRP are documented.	Inspected the Disaster Recovery Plan and determined that the policy was reviewed and approved on an annual basis. Inspected the Disaster Recovery test and determined that the DRP was tested on an annual basis.	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
1	The DoControl Board of Directors meets quarterly and has a fixed agenda. The board establishes oversight responsibilities, applies relevant expertise and operates independently from management.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The DoControl management meets at least quarterly. The management meeting discusses operations, marketing and product issues.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a quarterly basis and that meeting minutes were retained.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and are available to DoControl's employees within the DoControl shared drive.	Inspected the policies and determined that policies were documented, reviewed and approved by management on an annual basis. Inspected the DoControl shared drive and determined that policies were available to employees.	No deviations noted.
9	New employees are required to sign a standard employment agreement outlining confidentiality and 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.
55	Customers' passwords/authentication tokens are encrypted.	Inspected the external tool configuration and determined that customer passwords were encrypted according to the DoControl security policy	No deviations noted.
58	Data at rest is encrypted.	Inspected the encryption configuration and determined that data at rest was encrypted.	No deviations noted.
59	New vendors, business partners and subcontractors are required to sign an agreement containing a confidentiality clause.	Inspected examples of signed business partners agreements and determined that the agreements contained a confidentiality clause.	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
56	Upon customer request at the end of an agreement, DoControl will dispose of customer confidential information.	Inspected the service termination procedure and determined that it outlined the steps to undertake if a client requested to have their confidential information disposed of. During the audit period, this situation did not occur.	No deviations noted.

****