Doorway

System and Organization Controls
SOC 2 Type I Report

As of August 15, 2022

REPORT ON CONTROLS PLACED IN OPERATION AT DORWAY LTD. RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY WITH THE INDEPENDENT SERVICE AUDITOR'S REPORT

TABLE OF CONTENTS

Doorway

Section I – Dorway Ltd. Management Assertion

Dorway Ltd.'s Management Assertion

September 30, 2022

We have prepared the accompanying "Description of the Doorway Platform (System), related to Security, Availability and Confidentiality as of August 15, 2022" (Description) of Dorway Ltd. (Service Organization) in accordance with the criteria for a description of a Dorway Ltd.'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 Doorway Platform (System) that may be useful when assessing the risks from interactions with the System as of August 15, 2022, particularly information about system controls that Dorway Ltd. 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).

Dorway Ltd. uses Heroku and Amazon Web Services (AWS) to provide infrastructure management services. The Description includes only Dorway Ltd.'s controls and excludes controls of Heroku and AWS. The Description also indicates that certain trust services criteria specified therein can only be met if Heroku's and AWS' controls assumed in the design of Dorway Ltd.'s controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of Heroku and AWS.

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 Dorway Ltd.'s controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

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

a. The Description presents the System that was designed and implemented as of August 15, 2022, in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls and the subservice organization applied the controls assumed in the design of Dorway Ltd.'s controls as of August 15, 2022.

Hugh Fraser

Co-Founder, Managing Partner & CISO

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

Independent Service Auditor's Report

To the Management of Dorway Ltd.

Scope

We have examined Dorway Ltd.'s accompanying "Description of the Doorway Platform (System), related to Security, Availability and Confidentiality as of August 15, 2022" (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria) and the suitability of the design of controls included in the Description as of August 15, 2022 to provide reasonable assurance that Dorway Ltd.'s service commitments and system requirements would be 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).

Dorway Ltd. uses Heroku and Amazon Web Services (AWS) (subservice organization) 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 Dorway Ltd., to achieve Dorway Ltd.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Dorway Ltd.'s system; its controls relevant to the applicable trust services criteria; and the types of complementary subservice organization controls that the service organization assumes have been suitably designed and implemented at Heroku and AWS. Our examination did not extend to the services provided by Heroku and AWS and we have not evaluated whether the controls management assumes have been implemented at Heroku and AWS have been implemented or whether such controls were suitably designed and operating effectively as of August 15, 2022.

The Description also indicates that Dorway Ltd.'s controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Dorway Ltd.'s controls are suitably designed and implemented, 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.

Dorway Ltd.'s responsibilities

Dorway Ltd. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service commitments and system requirements were achieved. Dorway Ltd. has provided the accompanying assertion titled, Dorway Ltd. management assertion (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design 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 if operating effectively. Dorway Ltd. is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed 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 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 to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved, if operating effectively, 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 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 would achieve its service commitments and system requirements based on the applicable trust services criteria if the controls operated effectively.
- Assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed 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 Description, or conclusions about the suitability of the design 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.

Other matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description, and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects:

a. The Description presents the Doorway Platform system that was designed and implemented as of August 15, 2022 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed as of August 15, 2022, to provide reasonable assurance that Dorway Ltd.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of August 15, 2022.

Restricted use

This report is intended solely for the information and use of Dorway Ltd., user entities of Dorway Ltd.'s Doorway Platform system as of August 15, 2022 and prospective user entities, independent auditors and practitioners providing services to such user entities who have sufficient knowledge and understanding of the following:

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

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

Kost Forer Gabbay and Kasierer

Kost Forer Gabbay and Kasierer
A member firm of Ernst & Young Global
September 30, 2022

Section III – Description of the Doorway Platform relevant to Security, Availability and Confidentiality as of August 15, 2022

Company Overview and Background

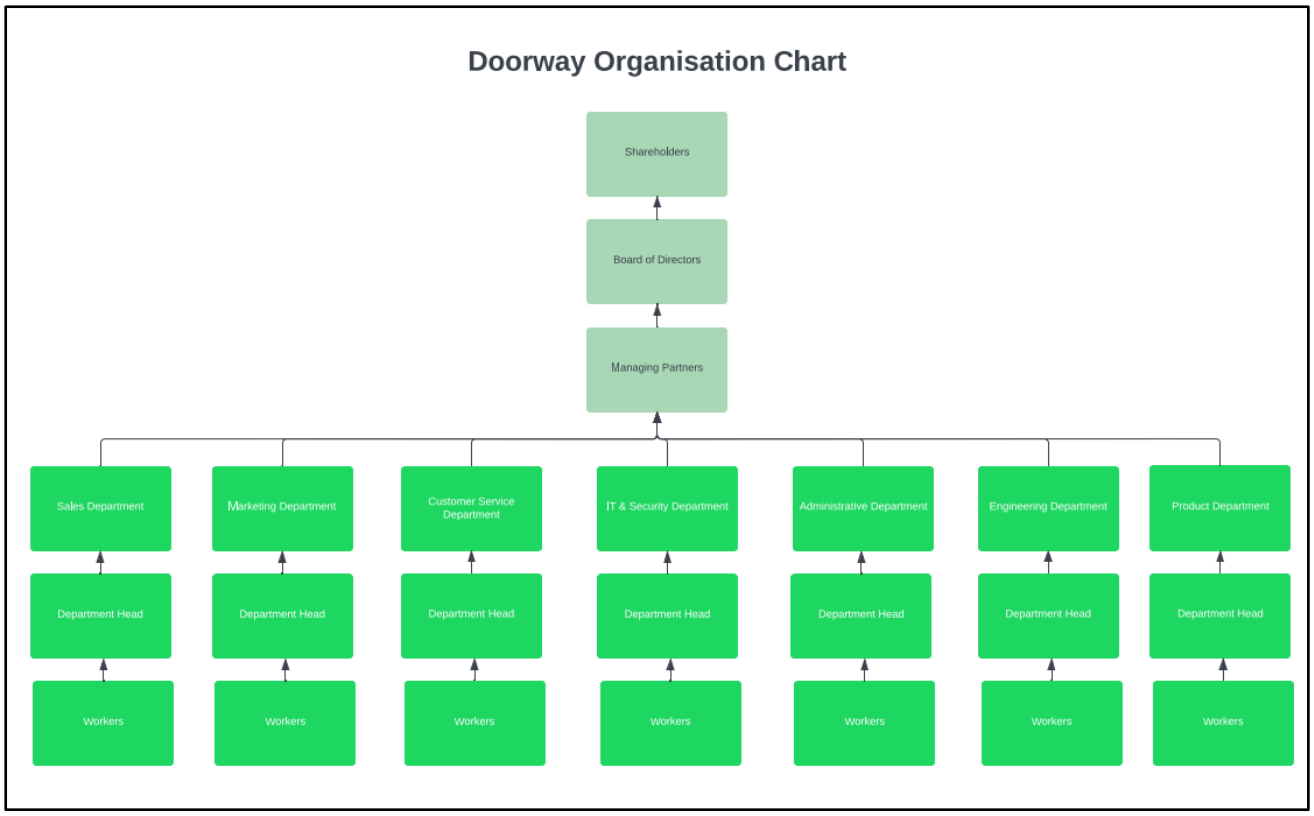
Doorway is a digital business card software service made for companies. Doorway is created with the intention to help companies move away from unsustainable paper business cards and to help improve the in-person networking efficiency of their employees.

Purpose and Scope of the Report

The scope of this report is limited to the controls supporting the Doorway and products and does not extend to other available software products and services or the controls at third third-party service providers.

Organizational Structure

Doorway's organizational structure provides the overall framework for planning, directing and controlling operations. It utilizes an approach whereby personnel and business functions are segregated into departments according to job responsibilities, lines of reporting and communications, and allows employees to focus on the specific business issues impacting their customers. Below is a description of key Doorway's departments:



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

Business Development & Managing Partnership*:* The business development & managing partnership department is responsible for identifying, building and managing partnerships with third-party entities.

Marketing: The marketing department is responsible for building the company's brand, generating sales opportunities, and other marketing activities.

Technical Services: The TS and operation department includes the following entities:

- *Information Technology (IT)*: The IT department is responsible for providing Doorway with the required IT environments.
- *Security:* The Security department is responsible for the production SaaS environments availability, security and scalability. It operates the NOC that provides 24x7 control, monitoring and resolution in case of failure.

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

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

Research & Development (R&D): The R&D department is responsible for developing, testing and validating Doorway's products and the business services implemented within the production environment.

Finance & Admin Team: The Finance and Admin department is responsible for the company's legal, financial and control activities including financial planning and administrative tasks.

Overview of Company's Internal Control

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

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. Doorway's executive management recognizes its responsibility for directing and controlling operations and for establishing, communicating and monitoring control policies and procedures. Policy and procedures documents for significant processes that address system requirements and relevant updates are available on the internal network.

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

Board of Directors - The Board of Directors (BOD) of Doorway is comprised 3 directors of which 2 are founders of the Company, who also serve as executive officers of the Company, and 1 is a non-operational member who represents the investors as the 'Investor Director'. The Board of Directors is actively engaged in the governance of the Company and its strategic direction. Members of the Board meet on at least a quarterly basis to discuss matters pertinent to the Company and to review financial information. The Board's responsibilities include but are not limited to (1) monitoring the actual

performance of the Company through its financial results; (2) monitoring the Company's compliance with legal and regulatory requirements; (3) analysis of the budget vs actual results; (4) guiding the Company in the way it funds its operation; (5) approving arrangements with executive officers relating to their employment relationships with the Company, including, without limitation, employment agreements, severance agreements, change in control agreements and restrictive covenants and (6) approving equity-based compensation plans in which directors, officers or employees may participate.

Management Philosophy and Operating Style – There is a management to the Company that meets on at least an annual basis. The Management Team, chaired by the Managing Partners has been delegated by the Board the responsibility to manage Doorway and its business daily. Doorway is led by a team with proven ability in cyber security and code security customer solutions to the global market. In its role, the Management Team assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. The Management Team designs policies and communications so that personnel understand Doorway's objectives, know how their individual actions interrelate and contribute to those objectives and recognize how and for what they will be held accountable. The Management Team convenes on a weekly basis or more frequently if necessary. In addition, the Management Team convenes off-site on a half-year basis for strategic purposes.

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

Human Resources Policy and Practices – Human resource policies and practices relate to hiring, orienting, training, evaluating, promoting and compensating personnel. The competence and integrity of Doorway's personnel are essential elements of its control environment. The organization's ability to recruit and retain highly trained, competent and responsible personnel is dependent to a great extent on its human resource policies and practices. Teams are expected to adhere to the Doorway's policies that define how services should be delivered and products need to be developed. These are located on the Doorway network and can be accessed by relevant Doorway team members while communicating by email and Slack on an as-needed basis.

Commitment to Competence - Competence at Doorway is designed to (1) identify and hire competent personnel, (2) provide employees with the training and information they need to perform their jobs, (3) evaluate the performance of employees to determine their ability to perform job assignments, and (4) through the performance evaluation process, identify opportunities for growth and job performance improvement. New professional employees that join Doorway are required to attend an On-Boarding welcome session, which provides them with the necessary knowledge about the firm and general work procedures. In addition, background checks are performed for new employees as part of the recruitment process to review in detail their qualifications.

Additionally, Doorway's Team Leaders are responsible for training plans for their newcomers. A professional training for existing employees is typically done only for new tools. It is the manager's role to decide what training a particular employee requires as they relate to specific job requirements. An annual review for all employees takes place. Main review topics are: Job perception, performance feedback, and manager-employee open discussion. Currently this review is not based on quantitative objectives. The review is written and submitted in native language (per site). Salary increases depend on promotion as well as evaluation discussions.

Control Activities

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

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

Risk Assessment

Risk identification: The process of identifying, assessing and managing risks is a critical component of Doorway's internal control system. The purpose of Doorway's risk assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives. Risk analysis embodies identification of key business processes in which potential exposures of some consequence exist. Exposures defined by Doorway, considers both internal and external influences that may harm the entity's ability to provide reliable services. It includes (1) identifying information assets, including physical devices and systems, virtual devices, 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 vendors providing goods and service, business partners, customers, and others with access to the Doorway's information systems.

Risk assessment: Ongoing monitoring and risks assessment procedures are built into the normal recurring activities of Doorway 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, reduce, or share the risk. Managers of each department are regularly in touch with personnel and may question the accuracy of information that differs significantly from their knowledge of operations. The Management Team considers the significance of the identified risks by determining the criticality and impact of the risks.

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

Risk responses that address and mitigate risks are carried out. The Management Team considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities. The relevant business processes are thoroughly controlled using a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls. Financial impacts of the risks are also taken in consideration during the process. Doorway assesses the risks associated to their vendors and business partners on a periodic basis.

Fraud assessment: Controls are in place at Doorway in order to evaluate and monitor the risks of fraud. The assessment of fraud considers:

- Fraudulent reporting
- Possible loss of assets
- Incentives and pressures
- Corruption resulting from the various ways that fraud and misconduct can occur.
- How management and other personnel might engage in or justify inappropriate actions.

Information and Communication

Information and communication are an integral component of Doorway's internal control system. It is the process of identifying, capturing and exchanging information in the form and timeframe necessary to conduct, manage and control the organization’s operations. At Doorway, information is identified, captured, processed and reported by various information systems, as well as through conversations with clients, vendors, regulators and employees.

Weekly management meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls and other strategic initiatives. Senior executives who lead the meetings use information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to organization-wide security policies and procedures are usually communicated to the appropriate Doorway personnel via email messages and shared with appropriate audience through the use of the internal communication tool. Availability, confidentiality and security related obligations are communicated to Doorway's employees through the confidentiality and non-disclosure agreements while client obligations and commitments are communicated within the contracts. In addition, Doorway's approved policies as well as the process of informing the entity about breaches of the system Security, Availability and Confidentiality are communicated to personnel responsible for implementing them in the internal application.

General Company Policies

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

Monitoring

Managers at Doorway are responsible for monitoring the quality and effectiveness of the various operations and internal controls as a routine part of their activities. Performance reports and statistics are generated on a regular basis and presented to Executive management for evaluation. Management uses automated reports created through various applications and processes to monitor the efficiency of specific processes and the effectiveness of specific key controls. Metrics produced from these systems are used to identify the strengths and achievements, as well as the weaknesses, inefficiencies or potential performance issues with respect to a specific process. Managers have responsibility for informing their direct reports about these items at the appropriate time. The Executive Management Team monitors the progress with respect to Doorway’s service processes on a regular basis. Analysis of root cause is performed through various tools and meetings, and corrective measures are communicated to relevant groups through e-mails, meetings, and a project portal tool in order to prevent future occurrences.

Asset Management

Company assets are tracked and managed throughout the asset life cycle. Assets are assigned owners to ensure there is an individual responsible for securing the asset. The tracked assets include production components as well as employee

devices that may contain personal data. When assets reach end-of-life they are securely destroyed to ensure that data is not recoverable.

Logical and Physical Access

Doorway has established an organization-wide information security policy designed to protect information at a level commensurate with its value. The policy dictates security controls for media where information is stored, the systems that process it, as well as infrastructure components that facilitate its transmission. A security policy is documented by Doorway management, reviewed and approved on an annual basis.

Access Control, User and Permissions Management

Doorway builds its production environment system architecture using Heroku (hosted on Amazon Web Services) and AWS services. Firewall detailed configuration is defined and performed by the Doorway Operations team. In addition, the global management of the Doorway infrastructure is performed by Doorway using a dedicated Heroku and AWS workspace. This interface allows Doorway to, among others, (1) add, modify and manage servers, (2) create security policies as they relate to these servers, (3) configure a few network and firewall parameters, (4) manage the databases and (5) manage the Heroku and AWS users. Firewalls separate the internal network from the internet. Firewall settings have been configured to allow only authorized traffic, as defined in Doorway's Security Policy.

Doorway manages and delivers its services using a variety of systems and environments. As previously described, information security controls and procedures are implemented throughout these systems, to help prevent unauthorized access to data. Authorized access to the Heroku and AWS hosting environment is performed directly from the Doorway office or using VPN to the Doorway office then to servers' farm by using SAML authentication and two factors authentication. The database servers reside within the production environment. The access to the production environment servers is restricted to authorized personnel (refer to section ‘Production Environment Logical Access).

Recertification of Access Permissions

Doorway has implemented a recertification process to help ensure that only authorized personnel have access to the production interface, servers, environments and databases. Employees whose job functions have changed and therefore no longer require access to a group of user permissions will have their access disabled or modified as needed.

Revocation Process

Terminated employees complete a termination clearance process on their last day at Doorway while the termination notification is documented and accessible within the Doorway Internal IT management ticket system, Linear. This process includes revocation of access permissions to the systems and premises, as well as the return of the property, data and equipment.

Production Environment Logical Access

The production environment is separated into Virtual Private Cloud (VPC) which are assigned to customers. Access to the customer environment web application interface is performed using personal production username and password for relevant users. Admin access to the Heroku and AWS servers is performed using a VPN between Doorway's offices and the Heroku and AWS Data Centers, which is uniquely identified at the respective Heroku and AWS datacenters. This access still requires a specific production username and password, which is available to each relevant user. The access to the Production servers is performed by using SSH keys and is restricted to authorized personnel.

Employees are provided with the minimal access rights required to carry out their duties. New users accessing Doorway’s system are granted access upon notification from the HR department. A detailed ticket is opened in the IT management ticketing system using a new hire template. This template includes all user detailed permissions.

Remote Access

Doorway's internal networks are protected using commercial firewalls configured and administered by the IT department. In addition, Doorway's production environment servers are protected by the Heroku and AWS tools and controls configured by Doorway. Doorway employees are granted remote access to the internal production network environment based on the need-to-work principle. Traffic entering Doorway's production network is monitored and screened by a firewall and monitoring tools implemented by Heroku and AWS and configured by Doorway. Remote users are automatically disconnected from the production servers after a pre-defined period of inactivity and need to login again in order to re-establish connection to the network.

Physical Access and Visitors

Doorway recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures and controls have been implemented to help prevent unauthorized access to data, assets and restricted areas. These access cards are issued to Doorway's employees by the administrative manager. Permissions to issue cards and grant access are restricted to the administrative manager and the authorized designees.

Software Development Lifecycle (SDLC) Overview

The software development lifecycle consists of the following stages:

- Product/Engineering Requirements Definition
- Detailed Design
- Coding
- Unit Testing
- Integration Testing
- System Testing
- SAST scanning
- Beta Release
- General Availability (GA) Release

Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by the management team within the Change Management application. Each change goes through a life cycle. Product requirements are constantly being collected from customers and from market research by Doorway Product Managers. These requirements combined with additional engineering improvement requirements are discussed by R&D managers and Product Managers and are converted to a Product Requirements Document (PRD) that contains more specific description of required features and changes.

The R&D Managers review the PRD and provide a high-level effort estimation for every feature. The product managers work with the R&D managers to create a prioritized features list based on the effort estimation and required timeline of the release. The Release Manager collects the features list, validates the total effort vs teams foreseen progress and creates a release plan specifying integration dates, Feature Freeze and Code Freeze dates as well as the release date of 1st release candidate to PS.

R&D Engineers are engaged with ongoing enhancements of the product functionality. Each engineer implements Unit Testing to every new coded software module in accordance with Unit Tests guidelines document. Doorway performs unit testing using a dedicated tool. R&D engineer's check-in their respective code to a common source control system that provides extensive version tracking functionality and other software building abilities. All changes which are added to the Source Control contain information linking them to the relevant features and bugs. Code changes are reviewed along with the pull request performed by the developer. Unit Tests are maintained according to product changes and enhanced based on bugs that were detected in previous product versions. Check-in of code triggers Unit testing process and if passed successfully, a new build is created, and automated tests are executed on it.

Software Testing and QA Process: Doorway Quality Assurance (QA) is constantly involved from early development stages. Based on the PRD, QA creates internal test plans. Test plans are reviewed by Product Managers and by R&D Team Leader responsible for the feature design. Each build goes through an automated pass/fail sanity testing process during which it is determined if it is acceptable to commence a full QA cycle. A full QA cycle (Stabilization) includes regression and progression tests according to test plan documents. During this stage bugs are reported in TFS. Manual tests are performed by the QA team. Each bug is assigned to an R&D Engineer for resolving with severity and a target version. Bugs that were targeted to the current version are fixed and verified as closed or are reopened. During Code Freeze, only Show Stopper bugs are fixed by the engineers.

Software Release: The official release of a version from Doorway development should qualify by the Release Exit Criteria. It is mandatory that all automation tests pass and that scans are free of Critical and High findings. Doorway secured development process also includes a yearly pen testing of which findings are fixed in the following release. The released version is verified by the Professional Services (PS) prior to releasing to Beta customers. Show stopper bugs are reported and fixed in a new Release Candidate. A Beta version is released to selected customers. Customers who receive Beta version are notified in advance and express their wish to actively participate in this stage. The Beta version is used in standard operational environments of these customers. Bugs or functional requests that are made by customers are reported in TFS and marked with customer tag. Faults reported during this stage are analyzed by R&D and if defined as showstoppers, they will be fixed for the General Availability (GA) release. Requests for functional enhancements are going to Product Managers backlog for future Releases. A General Availability (GA) version is released as a complete installation package including Built-in help, Administration Guide and Release Notes documents. A "release exit" checklist is filled by Doorway before releasing a version to production.

Monitoring the Change Management Processes

A change management meeting is performed every week, to assess the risks identified and review changes required to the production environment. Action items are updated within as part of the process and change is approved only after review and assessment. In addition, metric reports are regularly issued to the Management Team in order to provide them with key indicators regarding the change management process.

Infrastructure Change Management Overview

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

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

Description of the Production Environment

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

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

AWS's web service interface (AWS Console) allows Doorway to obtain and configure capacity. It provides Doorway with control of computing resources and runs on AWS's computing environment. EC2 reduces the time required to obtain and

boot new server instances to minutes, allowing to quickly scale capacity, both up and down, as computing requirements change. The use of EC2 allows to:

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

Production Environment

The processes described below are executed within Doorway's production environment, which is hosted in Amazon Web Services (AWS) Virtual Private Cloud located globally. The facilities comply with standards of quality, security, and reliability that enable Doorway to provide its' services in an efficient and stable manner. All Doorway users who connect to the customers' VPCs for support purposes should login via a named workspace. All authentication is performed with a SAML provider. Customers' data is encrypted at test and in transfer. Access of Doorway personnel as well as customers is further restricted by IP filtering. The production environment is completely separated from the corporate environment and follows strict access and data processing procedures and processes. The environment is managed by a selected few Security personnel who use 2FA to connect using a dedicated AWS or Heroku workspace.

Note: Controls performed by the data center service providers are not included in the scope of this report.

Network Infrastructure

Robust network infrastructure is essential for reliable and secure real-time data communication between the Doorway cloud service components. To provide sufficient capacity, the Doorway network infrastructure relies on platforms provided by Amazon Web Services (AWS). To ensure appropriate network security levels, Doorway security standards and practices are backed by a multi-layered approach that incorporates practices for preventing security breaches, ensuring confidentiality, integrity and availability. Doorway's security model encompasses the following components:
Application layer security, including:

- Various authentication schemas such as multi-factor authentication (MFA), unique ID and complex password policy
  - Logical security
  - Penetration testing
  - IP address source restriction
  - Customers' data encryption at-rest and in transit
- Network and infrastructure security, including:
  - Network architecture
  - Risk management
  - AWS data centers
  - Cloud operation security (change management, monitoring and log analysis)

Web, Application and Service Supporting Infrastructure Environment

Doorway utilizes AWS's clustered infrastructure design to provide redundancy and high availability. In addition, the infrastructure is configured in a way that enables auto scaling capabilities. This allows supporting high performance during demand spikes to the services.

Production Monitoring

Doorway uses a suite of monitoring tools to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules. Doorway's production network encompasses numerous components including web services, application

and data server types, database, monitoring tools, and redundant network equipment provided as part of the AWS services. In addition, to improve service availability to clients and to support the operations of the Doorway environments, Doorway maintains a dedicated Security department. The Security department is responsible for the ongoing work on the production environment as well as investigating escalated issues. The production environment, including the servers and application, is monitored 24/7/365 by the NOC and Security team. Key Doorway staff members are notified of events related to the security, availability or confidentiality of service to clients.

Security and Architecture

Doorway provides a secure, reliable and resilient Software-as-a-Service platform that has been designed from the ground up based on industry best practices. The below addresses the network and hardware infrastructure, software and information security elements that Doorway delivers as part of this platform, database management system security, application controls and intrusion detection monitoring software.

Data Center Security

Doorway relies on Amazon Web Services global infrastructure, including the facilities, network, hardware, and operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of basic computing resources and storage. This infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards: FedRAMP, HIPAA, ISO 27001:2015, AICPA SOC 1, SOC 2, SOC 3 and PCI-DSS and more. The environmental protection managed by the vendors policies are:

- **Redundancy** - The data centers are designed to anticipate and tolerate failure while maintaining service levels with core applications deployed to multiple regions.
- **Fire Detection and Suppression** – Automatic fire detection and suppression equipment has been installed to reduce risk.
- **Redundant Power** – the data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and Uninterruptable Power Supply (UPS) units provide back-up power in the event of an electrical failure. Data centers use generators to provide back-up power for the entire facility.
- **Climate and Temperature Controls** – maintain a constant operating temperature and humidity level for all hardware.
- **Physical access** - AWS recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures and controls have been implemented to help prevent unauthorized access to data, assets and restricted areas.

Infrastructure Security

- **End-to-End Network Isolation** - the Virtual Private Cloud is designed to be logically separated from other cloud customers and to prevent data within the cloud being intercepted.
- **External & Internal enforcement points** - All servers are protected by restricted AWS firewall rules. The configuration of AWS firewall rules is restricted to authorized personnel.
- **Server Hardening** - all servers are hardened according to industry best practices.
- **Segregation Between Office and Production Networks** – there is a complete separation between the Doorway Corporate network and the Production network. Access to the production environment is granted to authorized personnel only, and traffic between the networks is sent over an encrypted tunnel.

Application Security

- **Penetration Testing** - The penetration tests include, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own. In addition, security scans are performed on a semi-annual basis. The penetration tests and security scans are performed by a reputable third-party vendor.
- **Vulnerabilities Management** - Web application architecture and implementation follow OWASP guidelines. The application is regularly tested for common vulnerabilities (such as CSRF, XSS, SQL Injection).

- **Segregation of Customer Data** - Doorway employs a login system and authorization mechanism based on industry best practices. During each user request, a validation process is performed through encrypted identifiers to ensure that only authorized users gain access to the specific data. The process is validated by third-party security consultants on a yearly basis.

Operational Security

- **Configuration and Patch Management** – Doorway employs a centrally managed configuration management system, including infrastructure-as-code systems through which predefined configurations are enforced on its servers, as well as the desired patch levels of the various software components.
- **Security Incident Response Management** - Whenever a security incident of a physical or electronic nature is suspected or confirmed, Doorway's engineers are instructed to follow appropriate procedures. Customers and legal authorities will be notified as recurred by Privacy regulations.
- **Antivirus** - Anti-virus definition updates are performed and monitored on a regular basis by the IT and Operations teams. The employees' laptops are encrypted with the use of a 256-bit AES encryption.
- **Unified Endpoint Management** - Doorway use a dedicate tool that implemented an Agent in advance on the company's endpoint in order to monitor and control the updates, data, content, configuration and encryption of the asset. The company Security Policy is enforced using a dedicate tool.

Human Resource Security

- **Security Awareness Training** - Doorway's employees undergo an information security awareness training upon joining the company, as well as periodically in conformance to Doorway's information security policy. The training ensures that each group of employees receive security training according to its technical knowledge and its needs.
- **Secure Coding Standards and Training** - Doorway's R&D team is regularly trained in secure coding practices such as CERT Oracle Secure Coding Standard for Java and the OWASP top 10. Furthermore, it is involved with analyzing penetration test results and defining the 'lessons learned'.

Support

Doorway's customer support procedures are designed to handle and resolve issues and requests in a timely manner. This includes issues that are internally identified, or issues submitted by clients. Doorway provides its clients with two types of support. Doorway customers choose either the Standard Support level or the Premium Support level. All three types are available 24/7/365 via support mail, support hotline and customer support portal.

Ticketing and Management

Doorway opens a ticket when an issue is raised by a client or when an issue is proactively identified. Doorway uses a third-party CRM application to manage, classify and ticket the client support-related issues. Tickets are classified by the level of urgency and assigned to the appropriate support tier for resolution.

Incident Management Process

A help-desk application is available to Doorway employees to report breaches in system security, availability, and confidentiality. New employees are trained in the use of this application at the beginning of their employment. The process is initiated when a new ticket is submitted in the helpdesk application or through emails. The company has a procedure and process in place to raise and manage Information Security Incidents. Incidents are classified according to the level of urgency and importance. Incidents can be submitted into the system following a customer-identified issue, through both manual and automated proactive checks, or automatically through an email request. The application has pre-defined steps that are assigned to a pre-defined group of employees. The completion of each step is recorded in the application. When an incident is submitted, an email is sent to the IT and Information Security Director. Resources are allocated to investigate the incident and resolve the issue. The IT and Information Security Director is responsible for

escalating critical incidents and perform Lesson Learnt reviews. By procedure and according to a strict SLA, Incident notifications are sent to customers in the case that their data has been impacted.

Escalation Process

Doorway's goal is to resolve issues in an efficient manner. The issue is tracked and updated in the support ticketing system. The escalation process is defined and documented by Customer Support. Tickets are escalated as deemed necessary to Security, R&D or Technical Services teams. Service interruptions are communicated to clients using e-mail based on the escalation procedures and Service Level Agreement (SLA) notification thresholds. In addition, to maintain visibility on current support issues and potential problem trends, support metrics (including Key Performance Indicators) are generated from the support application and sent to Company's stakeholders on a regular basis.

Availability Procedures

Doorway's production environment is fully managed as part of the AWS and Heroku services and monitored by Doorway Operation team using the tools provided by AWS and Heroku as well as internal tools. The application level is fully managed by the Doorway Security team. Doorway has implemented the operations management controls described below to manage and execute production operations.

Database Backup

Doorway's databases are hosted on AWS and fully backed up daily. The backup system automatically generates a backup log. In case of failure, a notification is sent to the Operation team. The company hold replicas to each data center for high-availability standards in case of a disaster.

Restoration

Backup data captured as part of the daily, weekly and monthly backup procedures is restored automatically into a separate environment in order to determine the integrity of data and potential data recovery issues. A log of the restoring process is sent to the Director of Operations for review.

Data center availability procedures

Heroku and AWS provides Doorway with a secured location implementing security measures to protect against environmental risks or disaster.

Business Continuity Plan (BCP)

Doorway has developed a Business Continuity Plan to enable the company to continue to provide critical services in case of a disaster. Doorway maintains a backup server's infrastructure at a separate location within the Heroku and AWS environments. The backup server's infrastructure has been designed to provide clients with business-critical services until the disaster has been resolved and the primary system is fully restored. The alternative processing environment is wholly managed by appropriate Doorway personnel, as is the case with the primary production environment.

Monitoring Usage

The management team is updated on an annual basis on security, confidentiality and availability non-compliance issues that may come up and address them as needed. Such issues are documented as part of a support process and if necessary, notifications are sent to the Security team or the IT and Information Security Director. Change reports, vulnerability reports from production and monitoring tools as well as support metrics are reviewed and discussed in relation to organization's system security, availability and confidentiality policies. In addition, environmental, regulatory and technological changes are monitored. Their effects are assessed, and their policies are updated accordingly. A summarized protocol is made available to relevant managers and team members.

Confidentiality Procedures

Customer confidentiality is key factor in Doorway. As such, Doorway has implemented security measures to ensure the confidentiality of its customer's sensitive personal information. The security measures aim to prevent unauthorized access, disclosure, alteration or destruction of sensitive personal information. In addition, connections to the Doorway network and databases are obtained through a secured IPSEC tunnel, only accessible from within the production network.

Data Encryption

- **Data in transit** - all traffic between the customer and the Doorway platform is encrypted through TLS with only the most secure algorithms enabled. Encryption between Doorway customers and the Application as well as between Doorway sites is enabled using an authenticated TLS tunnel. Connections to the Doorway network and databases are obtained through a secured IPSEC tunnel, only accessible from within the production network. Clients' sessions and interactions are encrypted using 256bit SSL V3/TLS HTTPS. Internet traffic is encrypted using high class level certificates based on the PKI infrastructure. Doorway uses encryption to supplement other measures used to protect data-at-rest when such protections are deemed appropriate based on assessed risk. Processes are in place to protect encryption keys during generation, storage, use, and destruction.
- **Data at rest** - Encrypted based on AWS's data at rest encryption policies which adhere to the following: Several layers of encryption to protect customer data at rest in Amazon Web Services products. Data stored in AWS is encrypted at the storage level using AES256 Customer content stored at rest is encrypted, without any action required from the customer, using one or more encryption mechanisms. Data for storage is split into chunks, and each chunk is encrypted with a unique data encryption key. These data encryption keys are stored with the data, encrypted with ("wrapped" by) key encryption keys that are exclusively stored and used inside Amazon's central Key Management Service. Amazon's Key Management Service is redundant and globally distributed. A common cryptographic library is used to implement encryption consistently across almost all Google Cloud Platform products. Because this common library is widely accessible, only a small team of cryptographers needs to properly implement and maintain this tightly controlled and reviewed code.

Subservice Organizations Carved-out Controls: Heroku and Amazon Web Services ('AWS')

The subservice organization is expected to:

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

Dorway Ltd.'s Customers' Responsibilities

- Implementing sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with Dorway Ltd.

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

Description of Criteria and Controls

Control Environment

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

#	Controls specified by the Company
37	Doorway has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to employees. Employees must accept the Acceptable Use Policy upon hire.
44	Doorway has a formal Code of Conduct approved by management and accessible to employees. Employees must accept the Code of Conduct upon hire.
40	Doorway requires its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.
32	Doorway Management has approved general policies and procedures, and employees accept these procedures when hired. Management also ensures that security policies are accessible to employees and contractors.
39	Doorway's new hires are required to pass a reference check as a condition of their employment.

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
16	Doorway conducts a Risk Assessment at least annually. Doorway's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
146	The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.

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
14	Doorway reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.

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
38	Doorway evaluates the performance of employees through a formal, annual performance evaluation.
44	Doorway has a formal Code of Conduct approved by management and accessible to employees. Employees must accept the Code of Conduct upon hire.
40	Doorway requires its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.
47	Doorway positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Doorway.
39	Doorway's new hires are required to pass a reference check as a condition of their employment.
36	Doorway has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Doorway's security policies and procedures, including the identification and reporting of incidents. Full-time employees are required to complete the training upon hire and annually thereafter.

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
37	Doorway has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to employees. Employees must accept the Acceptable Use Policy upon hire.
38	Doorway evaluates the performance of employees through a formal, annual performance evaluation.
44	Doorway has a formal Code of Conduct approved by management and accessible to employees. Employees must accept the Code of Conduct upon hire.
36	Doorway has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Doorway's security policies and procedures, including the identification and reporting of incidents. Full-time employees are required to complete the training upon hire and annually thereafter.

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
16	Doorway conducts a Risk Assessment at least annually. Doorway's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
21	Doorway maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control. Management performs an annual review.
153	Doorway performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.
160	Doorway conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
53	Doorway has an established policy and procedures that governs the use of cryptographic controls.
13	Doorway has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.
2	Doorway authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.

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
37	Doorway has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to employees. Employees must accept the Acceptable Use Policy upon hire.
44	Doorway has a formal Code of Conduct approved by management and accessible to employees. Employees must accept the Code of Conduct upon hire.
160	Doorway conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
9	Doorway provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.

#	Controls specified by the Company
32	Doorway Management has approved general policies and procedures, and employees accept these procedures when hired. Management also ensures that security policies are accessible to employees and contractors.
159	Doorway has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing. Doorway has identified an incident response team that prioritises and monitors incidents. The response team tracks incident resolution and lessons learnt.
36	Doorway has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Doorway's security policies and procedures, including the identification and reporting of incidents. Full-time employees are required to complete the training upon hire and annually thereafter.

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

#	Controls specified by the Company
64	Doorway's security commitments are communicated to external users, as appropriate.
74	Doorway communicates system changes to customers that may affect security, availability, processing integrity, or confidentiality.
8	Doorway provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.
159	Doorway has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing. Doorway has identified an incident response team that prioritises and monitors incidents. The response team tracks incident resolution and lessons learnt.
66	Doorway maintains a Terms of Service that is available to external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems. Client Agreements or Master Service Agreements are in place for when the Terms of Service may not apply.
24	Doorway tracks incidents through internal tools and closes them within an SLA that management has pre-specified.
56	Doorway maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.
57	Doorway maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.

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
19	Doorway engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.
16	Doorway conducts a Risk Assessment at least annually. Doorway's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
18	Doorway engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.
15	Doorway has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.

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
16	Doorway conducts a Risk Assessment at least annually. Doorway's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
18	Doorway engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.
15	Doorway has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.
56	Doorway maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.
57	Doorway maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.

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
16	Doorway conducts a Risk Assessment at least annually. Doorway's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.

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
19	Doorway engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.
16	Doorway conducts a Risk Assessment at least annually. Doorway's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
14	Doorway reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.
18	Doorway engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.
56	Doorway maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.

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
11	Doorway performs annual access control reviews.
19	Doorway engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.
16	Doorway conducts a Risk Assessment at least annually. Doorway's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
18	Doorway engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.
56	Doorway maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.

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
19	Doorway engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.
16	Doorway conducts a Risk Assessment at least annually. Doorway's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
159	Doorway has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing. Doorway has identified an incident response team that prioritises and monitors incidents. The response team tracks incident resolution and lessons learnt.
18	Doorway engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.
56	Doorway maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.

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
19	Doorway engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.
16	Doorway conducts a Risk Assessment at least annually. Doorway's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
160	Doorway conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
14	Doorway reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.
18	Doorway engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.

#	Controls specified by the Company
15	Doorway has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.

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
19	Doorway engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.
16	Doorway conducts a Risk Assessment at least annually. Doorway's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
160	Doorway conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
53	Doorway has an established policy and procedures that governs the use of cryptographic controls.
32	Doorway Management has approved general policies and procedures, and employees accept these procedures when hired. Management also ensures that security policies are accessible to employees and contractors.
2	Doorway authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.
18	Doorway engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.
36	Doorway has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Doorway's security policies and procedures, including the identification and reporting of incidents. Full-time employees are required to complete the training upon hire and annually thereafter.

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
26	Doorway conducts annual BCP/DR tests and documents according to the BCDR Plan. Doorway has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.
44	Doorway has a formal Code of Conduct approved by management and accessible to employees. Employees must accept the Code of Conduct upon hire.

#	Controls specified by the Company
9	Doorway provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.
32	Doorway Management has approved general policies and procedures, and employees accept these procedures when hired. Management also ensures that security policies are accessible to employees and contractors.
13	Doorway has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.
15	Doorway has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.

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
58	Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for external users, and MFA required for employee users.
93	Doorway has an established key management process in place to support the organization's use of cryptographic techniques.
54	Doorway stores customer data in databases that is encrypted at rest.
52	Doorway ensures that company-issued laptops have encrypted hard-disks.
67	Doorway requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.
49	Doorway ensures that a password manager is installed on company-issued laptops.
68	Doorway has established formal guidelines for passwords to govern the management and use of authentication mechanisms.
60	Doorway's application user passwords are stored using a salted password hash.

#	Controls specified by the Company
59	Role-based security is in place for internal and external users, including super admin users.
69	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.
71	Access to corporate network, production machines, network devices, and support tools requires a unique ID.
90	Doorway does not use Root Account on Infrastructure provider

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
63	External users must accept the Terms of Service prior to their account being created.
11	Doorway performs annual access control reviews.
69	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.
70	Access to infrastructure and code review tools is removed from terminated employees within one business day.
43	A termination checklist is used to ensure that system access, including physical access, for terminated employees has been removed within one specified time
71	Access to corporate network, production machines, network devices, and support tools requires a unique ID.

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
63	External users must accept the Terms of Service prior to their account being created.
11	Doorway performs annual access control reviews.
59	Role-based security is in place for internal and external users, including super admin users.
69	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.
70	Access to infrastructure and code review tools is removed from terminated employees within one business day.
43	A termination checklist is used to ensure that system access, including physical access, for terminated employees has been removed within one specified time
71	Access to corporate network, production machines, network devices, and support tools requires a unique ID.

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
11	Doorway performs annual access control reviews.
94	Doorway has security policies that have been approved by management and detail how physical security for the company's headquarters is maintained. These policies are accessible to employees and contractors.
43	A termination checklist is used to ensure that system access, including physical access, for terminated employees has been removed within one specified time
56	Doorway maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.

#	Controls specified by the Company
57	Doorway maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.

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
43	A termination checklist is used to ensure that system access, including physical access, for terminated employees has been removed within one specified time

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

#	Controls specified by the Company
58	Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for external users, and MFA required for employee users.
75	Read/Write access to cloud data storage is configured to restrict public access.
91	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected
48	Doorway ensures that company-issued computers use a screensaver lock with a timeout of no more than 15 minutes.
67	Doorway requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.
68	Doorway has established formal guidelines for passwords to govern the management and use of authentication mechanisms.
55	Doorway ensures that connections to its web application from its users are encrypted.
72	SSH users use unique accounts to access production machines.
88	WAF in place to protect Doorway's application from outside threats.

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
54	Doorway stores customer data in databases that is encrypted at rest.
61	Doorway's customer data is segregated from the data of other customers
52	Doorway ensures that company-issued laptops have encrypted hard-disks.
55	Doorway ensures that all connections to its web application from its users are encrypted.
72	SSH users use unique accounts to access production machines.

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
87	Doorway has infrastructure logging configured to monitor web traffic and servers for suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.
50	Doorway requires antivirus software to be installed on workstations to protect the network against malware.
51	Doorway's workstations operating system (OS) security patches are applied automatically.
152	Doorway ensures that virtual machine OS patches are applied monthly.

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
19	Doorway engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.
5	When Doorway's application code changes, code reviews and tests are performed by someone other than the person who made the code change.
160	Doorway conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
91	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected
87	Doorway has infrastructure logging configured to monitor web traffic and servers for suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.
18	Doorway engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.

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
89	Doorway is using Drata to monitor the security and compliance of its cloud infrastructure configuration
91	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected
87	Doorway has infrastructure logging configured to monitor web traffic and servers for suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.
18	Doorway engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.

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
159	Doorway has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing. Doorway has identified an incident response team that prioritises and monitors incidents. The response team tracks incident resolution and lessons learnt.

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
159	Doorway has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing. Doorway has identified an incident response team that prioritises and monitors incidents. The response team tracks incident resolution and lessons learnt.

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

#	Controls specified by the Company
154	Doorway ensures that incident response plan testing is performed on an annual basis.
77	Doorway performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy. Doorway monitors the status of backups on a daily basis and action is taken when the backup process fails. An automated email is sent to appropriate personnel when the backup process fails. Failed backups are resolved in a timely manner.
159	Doorway has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing. Doorway has identified an incident response team that prioritises and monitors incidents. The response team tracks incident resolution and lessons learnt.

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
155	Doorway ensures that code changes are tested prior to implementation to ensure quality and security.

#	Controls specified by the Company
5	When Doorway's application code changes, code reviews and tests are performed by someone other than the person who made the code change.
6	Only authorized Doorway personnel can push or make changes to production code.
156	Doorway ensures that releases are approved by appropriate members of management prior to production release.
7	Separate environments are used for testing and production for Doorway's application
31	Doorway has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.

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
157	Doorway maintains cybersecurity insurance to mitigate the financial impact of business disruptions.
77	Doorway performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy. Doorway monitors the status of backups on a daily basis and action is taken when the backup process fails. An automated email is sent to appropriate personnel when the backup process fails. Failed backups are resolved in a timely manner.
159	Doorway has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing. Doorway has identified an incident response team that prioritises and monitors incidents. The response team tracks incident resolution and lessons learnt.
27	Doorway utilizes multiple availability zones to replicate production data across different zones.

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

#	Controls specified by the Company
134	Doorway provides vendors and third parties with information on how to report breaches to Doorway.

#	Controls specified by the Company
56	Doorway maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.
57	Doorway maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.

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
76	Doorway authorizes designated member(s) with the autonomy to validate, change, and release critical security patches and bug fixes, outside of the standard change management process, when absolutely necessary to ensure security standards and availability of the systems.
81	Doorway has implemented tools to monitor Doorway's databases and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.
96	Doorway uses a load balancer to automatically distribute incoming application traffic across multiple instances and availability zones.
95	Doorway monitors its processing capacity continuously in order to appropriately manage capacity demand and to enable the implementation of additional capacity to meet availability commitments.

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
26	Doorway conducts annual BCP/DR tests and documents according to the BCDR Plan. Doorway has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.
77	Doorway performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy. Doorway monitors the status of backups on a daily basis and action is taken when the backup process fails. An automated email is sent to appropriate personnel when the backup process fails. Failed backups are resolved in a timely manner.
27	Doorway utilizes multiple availability zones to replicate production data across different zones.

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

#	Controls specified by the Company
100	Doorway tests the integrity and completeness of back-up information on an annual basis.
26	Doorway conducts annual BCP/DR tests and documents according to the BCDR Plan. Doorway has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.
76	Doorway authorizes designated member(s) with the autonomy to validate, change, and release critical security patches and bug fixes, outside of the standard change management process, when absolutely necessary to ensure security standards and availability of the systems.
77	Doorway performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy. Doorway monitors the status of backups on a daily basis and action is taken when the backup process fails. An automated email is sent to appropriate personnel when the backup process fails. Failed backups are resolved in a timely manner.

Confidentiality

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

#	Controls specified by the Company
58	Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for external users, and MFA required for employee users.
106	Doorway has a clean desk policy in place to ensure that documents containing sensitive data are not in public areas or laying on unattended employee work areas
61	Doorway's customer data is segregated from the data of other customers
105	Doorway's new hire contracts include a non-disclosure agreement (NDA)
67	Doorway requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.
68	Doorway has established formal guidelines for passwords to govern the management and use of authentication mechanisms.
59	Role-based security is in place for internal and external users, including super admin users.

#	Controls specified by the Company
55	Doorway ensures that all connections to its web application from its users are encrypted.
78	Storage buckets that contain customer data are versioned.
69	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.
104	Doorway uses test data within test environments.

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

#	Controls specified by the Company
103	Doorway deletes customer data within 30 days of the customer terminating its contract.
78	Storage buckets that contain customer data are versioned.
43	A termination checklist is used to ensure that system access, including physical access, for terminated employees has been removed within one specified time

****