SOC 2 Type II Report

For the period November 1, 2023 to October 31, 2024

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

CONFIDENTIAL INFORMATION

The information contained in this report is confidential and shall not be duplicated, published, or disclosed in whole or in part, or used for other purposes, without the prior written consent of Port Io Ltd.

Table of contents

Section I – Port Io Ltd.’s Management Assertion

December 16, 2024

We have prepared the accompanying "Description of the Port Platform relevant to Security, Availability and Confidentiality throughout the period November 01, 2023 to October 31, 2024" (Description) of Port Io Ltd. (Service Organization) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria). The Description is intended to provide report users with information about the Port Platform (System) that may be useful when assessing the risks arising from interactions with the System , particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria*.

Carved-out Unaffiliated Subservice Organization: Port Io Ltd. uses Amazon Web Services ('AWS') to provide infrastructure management services. The Description indicates that complementary controls at AWS that are suitably designed and operating effectively are necessary, along with controls at Port Io Ltd. to achieve the service commitments and system requirements. The Description presents Port Io Ltd.’s controls and the types of complementary subservice organization controls assumed in the design of Port Io Ltd.’s controls. The Description does not disclose the actual controls at the carved-out AWS.

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

a. The Description presents the System that was designed and implemented throughout the period November 01, 2023 to October 31, 2024 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed throughout the period November 01, 2023 to October 31, 2024 to provide reasonable assurance that Port Io Ltd. service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively and if the carved-out subservice organization applied the controls assumed in the design of Port Io Ltd.’s controls throughout that period.

c. The Port Io Ltd. controls stated in the Description operated effectively throughout the period November 01, 2023 to October 31, 2024 to provide reasonable assurance that Port Io Ltd.’s service commitments and system requirements were achieved based on the applicable trust services criteria, if the carved-out subservice organization applied the controls assumed in the design of Port Io Ltd.’s controls throughout that period.

Yonatan Boguslavski

Yonatan Boguslavski, CTO

Section II - Independent service auditor's report

To the Management of Port Io Ltd.

Scope

We have examined Port Io Ltd.'s accompanying description titled "Description of the Port Platform relevant to Security, Availability and Confidentiality throughout the period November 01, 2023 to October 31, 2024" (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report*, (Description Criteria) and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period November 01, 2023 to October 31, 2024 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA Trust Services Criteria.

Carved-out Unaffiliated Subservice Organization: Port Io Ltd. uses 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 Port Io Ltd., to provide reasonable assurance that Port Io Ltd.'s service commitments and system requirements are achieved based on the applicable trust services criteria. The description presents Port Io 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 implemented, suitably designed, and are operating effectively at AWS. The Description does not disclose the actual controls at AWS. Our examination did not include the services provided by AWS and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period November 01, 2023 to October 31, 2024.

Complementary user entity controls: The Description indicates that Port Io 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 Port Io Ltd.'s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Port Io Ltd.'s responsibilities

Port Io 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 its service commitments and system requirements were achieved. Port Io Ltd. has provided the accompanying assertion titled, Port Io Ltd.'s Management Assertion (Assertion) about the presentation of the Description based on the Description Criteria and the suitability of design and operating effectiveness of controls stated therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. Port Io 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) selecting the trust services categories addressed by the engagement and stating the applicable trust services criteria and related controls in the Description; (5) identifying the risks that threaten the achievement of the service organization's service commitments and system requirements; and (6) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of design and operating effectiveness of controls stated 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 American Institute of Certified Public Accountants (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 stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period November 01, 2023 to October 31, 2024. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

Our examination was not conducted for the purpose of evaluating the performance or integrity of Port Io Ltd.'s AI services. Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of Port Io Ltd.'s AI services.

We are required to be independent of Port Io Ltd. and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. 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 presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria, is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

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

Opinion

In our opinion, in all material respects:

a. the Description presents the Port Platform system that was designed and implemented throughout the period November 01, 2023, to October 31, 2024, in accordance with the Description Criteria.

b. the controls stated in the Description were suitably designed throughout the period November 01, 2023 to October 31, 2024, to provide reasonable assurance that Port Io Ltd.'s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Port Io Ltd.'s controls throughout that period.

c. the controls stated in the Description operated effectively throughout the period November 01, 2023, to October 31, 2024, to provide reasonable assurance that Port Io Ltd. service commitments and system requirements were achieved based on the applicable trust services criteria [if the complementary subservice organization and user entity controls assumed in the design of Port Io Ltd.'s controls operated effectively throughout that period.

Restricted use

This report , including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Port Io Ltd., user entities of Port Io Ltd.'s Port Platform system during some or all of the period November 01, 2023 to October 31, 2024 and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators 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.
- internal control and its limitations.
- complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- 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

December 16, 2024
Tel-Aviv, Israel

Section III - Description of the Port Platform Relevant to Security, Availability and Confidentiality for the period November 1, 2023, to October 31, 2024

Company Overview and Background

Port io was founded in 2021 by Zohar Einy and Yonatan Boguslavski. Port io Ltd. is privately held with locations in Israel and backed by TLV Partners, Yoav Landman, and Hapri ltd.

Products and Services

Port is a Developer Platform made to make life easier for developers and DevOps in an organization by creating a single platform that acts as a single source of truth for all of the infrastructure assets and operations existing in the organization's tech stack.

Port then allows engineers to perform actions on these assets in a self-service fashion. From provisioning a dev environment, understanding who the owner of a microservice is, or any unique use case, DevOps wants to self-serve and automate.

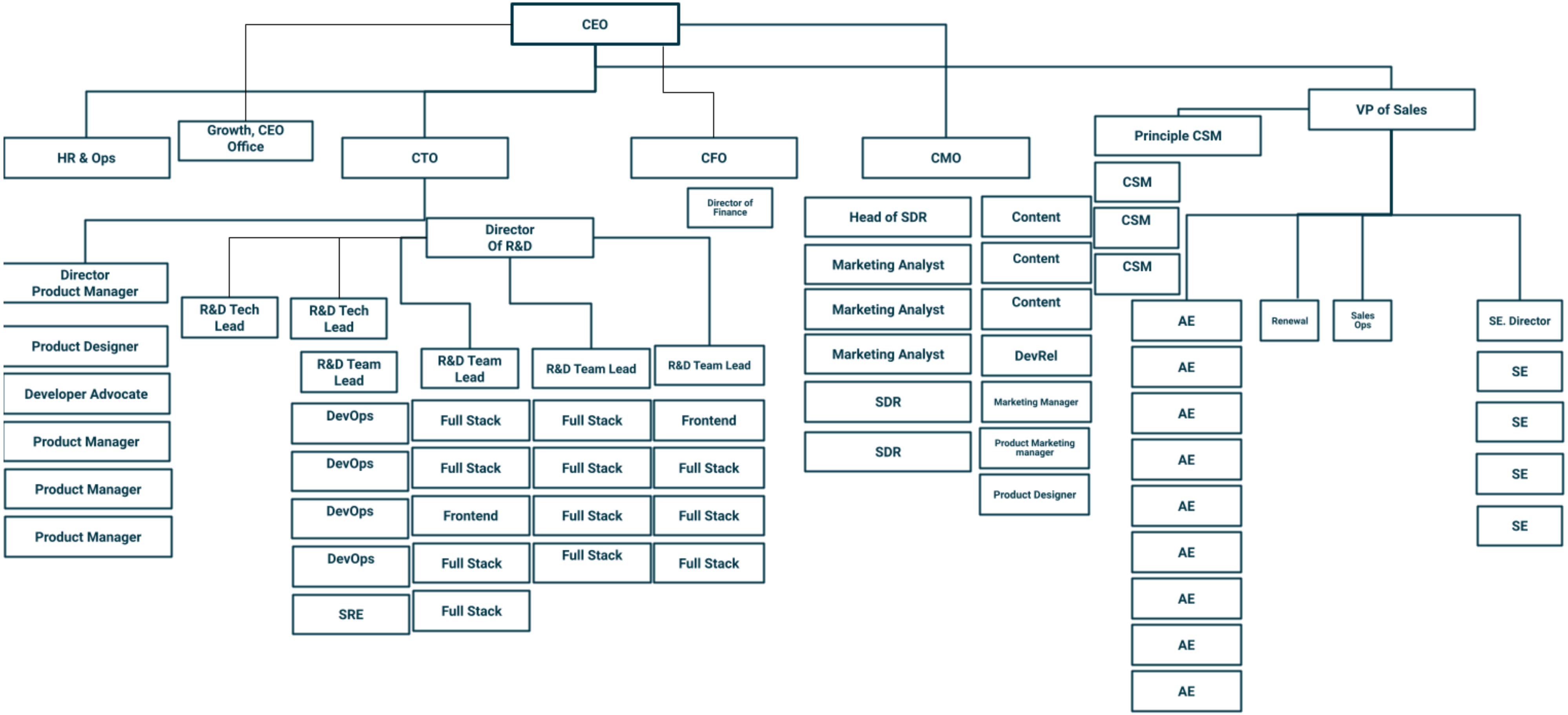
Purpose and Scope of the Report

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

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

Organizational Structure

Port's organizational structure provides the overall framework for planning, directing, and controlling operations by segregating duties between business functions. Port's Operations department receives supporting services from other Port departments, such as Research and Development (R&D), Sales, and Marketing. An organizational chart is documented and approved by management that clearly defines management authorities and reporting hierarchy (**3**).



Job Description and Responsibilities of the Operations Team:

CTO

- Provides leadership and develops objectives for the service department.
- Obtains funding for existing and future projects.
- Develops and directs the design and development of new products and improves existing products.
- Works with members of the senior management team to further departmental and company goals.
- Plans to support future growth and expansion.
- Takes ownership of projects to improve Port's operations.
- Builds a skilled and responsible Dev team.

DevOps

- Responsibility for Port's 24/7 multi-site cloud operations.
- Handles exceptions and operational requests in Port's production environment.
- Implements and uses monitoring tools.
- Automates configuration management and deployment.
- Builds, scales, and optimizes critical production systems.
- Builds out and maintains disaster recovery (DR) for Port's production environments.
- Ensures the security of Port's critical systems.
- Maintains continuously involved with the larger Dev community and contributes the best practices to Port.

Developer

- Takes part in the product design and planning phases.
- Develops complex systems and services that are deployed in production at scale.
- Fixes and improves existing software where required.
- Research new technologies.
- Analyzes and studies complex system requirements.

Overview of Company's Internal Control

The Board of Directors, management, and other personnel manage the process of internal control, which is 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. These are the six components of internal control at Port.

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for the components of internal control, providing discipline and structure. The protection of assets from unauthorized use or disposition is executed in accordance with management's authorization and customer instructions. Port's management maintains an internal control structure that monitors compliance with established policies and procedures. Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to Port's employees within the Port internal portal (**5**). The internal control structure is refreshed annually based on Port's assessment of the risks facing the organization.

Management sets the tone for the integrity, ethics, and competence of Port's employees, policies and procedures, risk management process and monitoring, and the roles of significant control groups. Below are the categories that define management's tone:

- **Authority and Responsibility** — Lines of authority and responsibility are clearly established throughout the organization and are communicated through Port's: (a) management operating style; (b) organizational structure; (c) employee job descriptions; and (d) organizational policies and procedures.

- **Corporate Governance and Strategy** – Port's control environment is influenced by its Board of Directors. The Board of Directors of Port consists of the CEO and the CTO, who bring many years of accumulated industry experience and expertise in various business aspects. The Board is actively involved in, and continually scrutinizes, the activities of Port's functional groups and acts with respect to its fiduciary responsibilities. Additionally, the Board raises questions and pursues key initiatives with management, as well as interacts periodically with the external auditors. The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda with (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features (**1**).

- **Management Philosophy and Operating Style** – The Management Team, chaired by the CEO, has been delegated by the Board the responsibility to manage Port and its business on a daily basis. The Management Team designs policies and communications so that personnel understand Port'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 of the company meets on at least a monthly basis to discuss on-going issues and updates (**2**).

- **Integrity and Ethical Values** – Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Management may remove or reduce inappropriate incentives, extraneous pressures, or opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. In addition, management communicates Port's integral values and behavioral standards to personnel through executive policy statements. The Board and management recognize their joint responsibility in fostering a strong ethical environment within Port to ensure that its business affairs are conducted with integrity and in accordance with high standards of personal and corporate conduct.

- **Human Resource Policies and Practices** – Human resource ("HR") policies include practices related to hiring, orienting, training, evaluating, counseling, promoting, and compensating personnel. An essential element of the control environment is the competence and integrity of Port's personnel. Job descriptions are documented and maintained within the Port website and on external tools. Candidates go through screening and appropriate reference checks (**7**). New employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses (**9**). Teams are expected to adhere to Port's global policies that define how services should be delivered. These policies are documented on Port's internal network and can be readily accessed by relevant Port team members.

- **Commitment to Competence** – Competence at Port is designed to (a) identify and hire competent personnel; (b) provide employees with the training and information they need; (c) evaluate the performance of employees to determine their ability to perform job assignments; and (d) identify opportunities for growth and job performance improvement through the performance evaluation process. New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different Port policies and work procedures (**8**). Personnel responsible for the design, development, implementation, and operation of systems affecting security, availability, confidentiality, undergo training on an ad-hoc basis (**11**).

Risk Assessment Process

The process of assessing risks is a critical component of Port's internal control system. Risks and threats are evaluated by Port's Risk Assessment team during a quarterly risk assessment meeting. The team reviews vulnerability reports and monitoring tools in relation to the organization's system security, availability, and confidentiality policies. In addition, the team monitors environmental, regulatory, and technological changes. Their effects are assessed, and their policies are updated accordingly. Once a year, the senior management reviews and approves the yearly risk assessment report.

Control Activities

Control activities are the policies and procedures that enable management directives to be carried out. Control activities, whether automated or manual, generally relate to the achievement of specific control objectives and are applied at various organizational and functional levels.

Information and Communication

Management implements various methods of internal communication to enable employees to understand their roles and responsibilities and to communicate important issues in a timely manner. These methods include orientation and training programs for new employees, regular meetings, email messages, and more.

General Company Policies

Port has established policies that govern the use of its information security systems. These policies are reviewed and approved annually by the management team. The policies apply to employees, contractors, and temporary employees alike. Port may update and amend these policies from time to time as circumstances and technologies develop.

It is the employee’s responsibility to be aware of and comply with these policies. Failure to observe these policies may result in disciplinary action, up to and including termination, whether or not it causes any liability or loss to the company, and it may be performed at the company’s discretion.

Communication

Internal communication

Management promotes effective communication within the organization. This involves producing and delivering messages and campaigns, facilitating intra-company dialogues, and establishing policies, processes, and procedures. These policies, processes, and procedures are communicated to employees through the company’s internal portal. New features are communicated to employees by release notes emails (**13**). A description of the Port system and its boundaries is documented and communicated to the relevant Port employees within the internal portal and to external users through Port's website (**4**).

External communication

External communication is defined as the transmission of information between the company and another entity in the company's external environment, such as customers, potential customers, suppliers, investors, shareholders, and society at large. New features are communicated to customers, if relevant, through emails, the website or directly through the account manager (**12**).

Port Operations - Criteria and Controls

The Trust Services Criteria and the controls that meet the criteria are listed in the Description of Criteria and Controls at the end of this document. The Port application and supporting control procedures are described using the following criteria:

- Port’s policies relevant to security, availability, and confidentiality
- Security procedures
- Software development lifecycle and infrastructure change management procedures
- Availability procedures
- Confidentiality procedures
- Monitoring procedures

Port’s management has specified controls to achieve these criteria. Note that certain Port customers may have contracted with additional service organizations in conjunction with the services provided by Port. The accompanying description includes only Port's controls, not the related controls of any other service organizations that Port or Port's customers may have contracted out.

Port's Policies Relevant to Security, availability and confidentiality and Privacy

Formal written policies for the trust principles and processes within the organization are developed and communicated so that personnel understand Port's objectives. The assigned policy owner updates the policy annually, and the policy is reviewed and approved by designated members of management. Significant components of these policies include:

- Security, availability, and confidentiality requirements of users
- Protection requirements, access rights, access restrictions, retention, and destruction
- Risk assessment
- Preventing unauthorized access
- Adding new users, modifying access levels, and removing users
- Assigning responsibility and accountability for system availability and confidentiality
- Assigning responsibility and accountability for system changes and maintenance
- Testing, evaluating, and authorizing system components before implementation
- Addressing how complaints and requests are resolved
- Identifying and mitigating security, availability, confidentiality, privacy breaches, and other incidents
- Training and other resources to support system security policies
- Handling of exceptions and situations not specifically addressed in policies
- Identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements
- Sharing information with third parties
- Recovering and continuing service in accordance with customer commitments or other agreements
- Monitoring system capacity

Description of the Production Environment

Production Environment

Port executes the processes described below by using a secure cloud service platform. The platform complies with standards of quality, security, and reliability that enable Port to provide its services efficiently and dependably. Port protects confidential information against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition, according to confidentiality commitments and requirements.

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

Network Infrastructure

A robust network infrastructure is essential for reliable and secure real-time data communication between Port's cloud service components. To provide sufficient capacity, Port's network infrastructure relies on a secure cloud service platform. To ensure a secure network, Port's standards and practices are backed by a multi-layered approach that incorporates practices for preventing security breaches and ensuring confidentiality, integrity, and availability.

Port's security components:

- Application layer security:
  - Various authentication schemas (multi-factor authentication (MFA), a unique ID, and a complex password policy)
  - Logical security
  - Penetration testing
  - IP address source restriction
  - Customer data encryption at rest and in transit

- Network and infrastructure security:
  - Network architecture
  - Risk management
  - AWS data centers
  - Cloud operation security (change management, monitoring, and log analysis)

Web, Application and Service Supporting Infrastructure Environment

Port utilizes a clustered infrastructure design to provide redundancy and high availability. In addition, the infrastructure enables auto-scaling capabilities. This allows high performance during demand spikes for the services. Uptime requirements are defined in the SLA agreement. The agreement is communicated to the customers as part of the contract (**22**).

Security and Architecture

Port provides a secure, reliable, and resilient Software-as-a-Service (SaaS) platform that has been designed from the ground up based on industry best practices. Below are the network and hardware infrastructure, software, and information security elements that Port delivers as part of this platform.

Data Center Infrastructure

Port relies on Amazon Web Services (AWS) global infrastructure, including the facilities, network, hardware, and operational software (e.g., host OS, virtualization software) 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 27001:2013, AICPA SOC 1, SOC 2, SOC 3, PCI-DSS, and more. AWS constantly updates its compliance programs. In addition, Port.io performs a review of the SOC 2 report of its third party infrastructure provider on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at Port.io to address the CUECs (**36**).

AWS Data Centers

AWS data centers serve the highest industry standards in perimeter, infrastructure, data, and environmental layers. The company evaluates its suppliers on a semi-annual basis to ensure that controls are implemented to conform with the company policy, monitoring and logging of data center access, surveillance and detection, device management, operational support systems, infrastructure maintenance, and governance and risk. AWS constantly updates its efforts and controls.

Data Centers – Physical Security

Access is scrutinized – AWS restricts physical access to people who need to be at a location for a justified business reason. Employees and vendors who need to be present at a data center have to first apply for access and provide a valid business justification. The request is reviewed by specially designated personnel, including an area access manager. If access is granted, it is revoked once the necessary work is completed.

Entry is controlled and monitored – Entering the Perimeter Layer is a controlled process. AWS staff entry gates with security officers and employs supervisors who monitor officers and visitors via security cameras. When approved individuals are on site, they are given a badge that requires multi-factor authentication and limits access to pre-approved areas.

AWS data center workers control - AWS employees who routinely need access to a data center are given permission to enter relevant areas of the facility based on their job function. But their access is regularly scrutinized. Staff lists are routinely reviewed by an area access manager to ensure each employee’s authorization is still necessary. If an employee does not have an ongoing business need to be at a particular data center, they have to go through the visitor process.

Monitoring for unauthorized entry - AWS is continuously watching for unauthorized entry on its property using video surveillance, intrusion detection, and access-log monitoring systems. Entrances are secured with devices that sound alarms if a door is forced or held open.

Environmental Protection

Redundancy - The data centers are designed to anticipate and tolerate failure while maintaining service levels with core applications deployed to an N+1 standard.

Fire Detection and Suppression – Automatic fire detection and suppression equipment have been installed to reduce risk.

Redundant Power – The data center electrical power systems are designed to be fully redundant and maintainable without impact on operations, 24 hours a day. Uninterruptable Power Supply (UPS) units provide backup power in the event of an electrical failure. Data centers use generators to provide backup power for the entire facility.

Climate and Temperature Controls – The data center maintains a constant operating temperature and humidity level for all hardware.

Port Offices

Physical access to the offices is restricted to authorized personnel using a personal identification card according to the physical access policy (**34**). Visitors to the Port office are accompanied while on premises (**35**).

Infrastructure Security

End-to-End Network Isolation - The Virtual Private Cloud is designed to be logically separated from other cloud customers in order to prevent data within the cloud from being intercepted.

Network Security - Access to system resources is protected through a combination of firewalls, VPNs, native operating system security, database management system security, application controls, and intrusion detection monitoring software (**30**). All servers are protected by restricted AWS Security Groups, allowing only minimally required communication to and from the servers. The configuration of AWS Security Groups is restricted to authorized personnel.

Server Hardening - Servers are hardened according to industry best practices.

Intrusion Detection – Actions performed on the production environment, including OS, DB and application are monitored, logged and reviewed. Alerts are triggered upon the identification of an anomaly (**23**).

Denial of Service (DoS) Protection – AWS security monitoring tools help identify several types of denial of service (DoS) attacks, including distributed, flooding, and software/logic attacks. When DoS attacks are identified, the AWS incident response is initiated. In addition to the DoS prevention tools, redundant telecommunication providers monitor each region as well as protect against the possibility of DoS attacks. In case of a DoS attack, an incident notification is sent to the designated group.

Segregation between Office and Production Networks – Access to the networked resources management platform is restricted to authorized personnel. Interactions between customers and the Port platform are performed by using an encrypted channel based on an authenticated SSL connection (**52**).

Penetration Tests – An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved (**38**). The penetration tests are performed by an internationally acclaimed information security consulting group.

Antivirus – Antivirus software is installed on workstations and laptops supporting such software. Port uses a centralized management tool in order to receive alerts of the antivirus status (**39**).

Application Security

Access Control – Access to Port's services is through an identity-protected web application with full SSL security. Only authorized members of a specific organization have access to the organization's data. Organization administrators can disable access for users at any time. The application implements strict a user access-control policy. For example, access to the source control tool is performed using MFA and is restricted to authorized personnel (**31**).

Data Encryption – All traffic between the customer's client and Port's platform is encrypted through TLS1.2 with only the most secure algorithms enabled. Encryption between Port's customers and the application, as well as between Port's sites, is enabled using an authenticated TLS tunnel. Customer passwords are encrypted within the database (**51**).

Vulnerabilities Management – Vulnerability scans are performed continuously using the source code tool as a part of the SDLC process (**37**).

Segregation of Customer Data – Port 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 annually by third-party security consultants.

Operational Security

Identity and Access Management – New employees are granted access to the different environments by a ticketing system process and subject to manager approval (**32**). Access to the AWS management interface is performed using MFA and is restricted to authorized personnel.

Password Policy – A password policy is implemented within the different systems. Users are identified through the use of a user ID/password combination using an SSO tool. Strong password configuration settings, where applicable, are enabled including: (1) forced password change at defined intervals, (2) a minimum password length, (3) a limit on the number of tempts to enter a password before the user ID is suspended, and (4) password complexity (**25**).

Recertification of Access Permissions – Port has implemented a recertification process to help ensure that only authorized personnel have access to the systems, environments, and databases. Permissions to the different environments (production, databases and applications) are reviewed, approved and documented by the Port.io management on an annual basis (**33**). A new user is granted access to the production environment once approved by the CTO within the Port internal application. The approved request, including the detailed permissions, is sent to the CTO, who sets up the new user accordingly. Access to the production environment and database is granted upon job requirements. Developers do not have access to the production and database environments. Specific developers can be granted access for specific projects. These accesses are logged and reviewed (**29**). Terminated employees who had access to the production environment have their permissions removed and company equipment returned in a timely manner (**28**).

Configuration and Patch Management – Port employs centrally managed configuration management systems, 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, Port's engineers are instructed to follow appropriate procedures detailed in the Security Incident Response Policy. Customers and legal authorities will be notified as required `by privacy regulations.

Data Encryption

Port uses AWS APIs to manage services either directly from applications or third-party tools (e.g., software development kits [SDKs] and AWS command-line tools). TLS sessions are established between the client and the specific AWS service endpoint, depending on the APIs used, and all subsequent traffic, including the SOAP/REST envelope and user payload, is protected within the TLS session. Customer data at rest is encrypted and hosted separately via secured storage services provided by AWS.

Security and Privacy Awareness Training

The protection of sensitive data and the maintenance of a high level of security awareness demand regular training of all employees to review handling procedures for sensitive information and hold periodic security awareness. Employees go through annual security awareness training based on the Port security policy (**10**). An information security policy is documented, reviewed and approved by Port management on an annual basis. The security policy is available to Port employees within the Port portal (**6**).

Software Development Lifecycle and Change Management (SDLC)

Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved within the change management application (**42**). Several groups are involved in the software development lifecycle and change management (SDLC) processes. In addition, changes that may affect system security, availability, and confidentiality, or privacy are communicated to management and users who will be affected. Privacy impact and risks are evaluated to ensure that those changes will be in accordance with privacy regulations.

Change Initiation

There is a documented change management policy. The policy is reviewed and approved on an annual basis (**41**). Changes are documented by opening a ticket within the SDLC application. Decisions to approve, reject, or prioritize requirements are made by the relevant personnel. Tickets in the change management tool are connected to the source control tool in order to link the request to the code change (**43**). The decisions are taken after reviewing the impact of the change t from different levels (e.g., security, availability, confidentiality, and privacy). Approved changes and associated development-related tasks are submitted in the SDLC app, and a developer is assigned to resolve the change. For each such task, a single or multiple "Pull Request" is submitted by a developer, and the developer updates the ticket status within the SDLC App to "Code Review".

"Pull Request" – Code Review

Code changes are reviewed along with the pull request performed by the team leader. The code review is documented on the source control tool. Code review is mandatory in order to continue in the SDLC process and deploy a version to the production environment (**44**). Once the change is resolved, automation tests are performed using a dedicated tool on a regular basis in order to identify issues within the application (**46**). When approved, the code is merged into the master branch. At this point, it's tested again by a set of acceptance tests to validate the merged code. When all tests are successfully completed, the master branch is ready for the release process. The system is configured to send alerts on test failures to the relevant stakeholders. A successful test status is required to continue in the SDLC process (**47**). Once the change is resolved and successfully merged into the master branch, the developer updates the ticket status within the SDLC app to "Done".

Deployment to Production

The access to the deployment tool required MFA and is restricted to authorized personnel (**27**). The permission to approve merge requests and to deploy is restricted to authorized personnel (**45**). Before deploying to production, the developer will follow the specific "Deployment Check Lists" steps that include all the tasks needed to be done prior to and after the deployment, including verifying acceptance of all QA tests. In addition, the developer will monitor the production environment to verify a successful deployment. Changes performed to the application are communicated to Port's customers through release notes published on the Port website.

Emergency Changes

Emergency changes may be performed when it is the only way to solve a problem disrupting the application's operation and services in a reasonable time. In this case, the development team will perform the necessary changes and then inform the relevant managers. After the change is completed, relevant personnel will determine a permanent course of action to solve the problem (e.g., whether to back out of the emergency fix or allow it to remain in effect).

Availability Procedures

Port hosts its production environment in the AWS region, located in North Virginia, US. The production environment is fully managed by Port's DevOps.

The production environment is comprised of numerous components, such as web services, application and data server types, databases, monitoring tools, and redundant network services. Port maintains a dedicated DevOps team to provide service availability to customers and to support the operations of the Port environment.

Port uses a suite of monitoring tools in order to monitor its service. The production environment, including the servers and application, is monitored by the Operation Team. Key Port personnel are notified of events related to the security, availability, or confidentiality of service to clients (**24**). In addition, the DevOps team is responsible for investigating escalated issues. Port recognizes that backup and maintenance of data are critical to the operations of Port's services. It is essential that industry best practices be followed to ensure that data is backed up on a regular basis and the integrity of the procedure is sound. The DevOps Team is also responsible for managing and backing up various types of service-related procedures.

Database Backup (DB)

Database servers at the data centers are located in secured locations with security measures implemented to protect against environmental risks or disasters. Port utilizes relational, as well as NoSQL, databases that manage backups, software patching, automatic failure detection, and recovery. The DB instances are configured on a private-facing subnet with no internet access. To architect for high availability, Port runs DB instances in several availability zones using Multi Availability Zones (AZ) deployment and utilizing AWS automatic provisioning to maintain a synchronous standby replica of their DB instances in different availability zones.

The primary DB instance is synchronously replicated across availability zones to the standby replica in order to provide data redundancy, failover support, and keep the system fully operational during system backups. Each AZ runs on its own physically distinct, independent infrastructure and is engineered to be highly reliable. Port databases are replicated in several availability zones (**49**).

In cases of planned database maintenance, DB instance failure, or infrastructure failure, Port's database infrastructure allows failover (Disaster Recovery) to the standby site so that they can resume database operations as soon as the failover is complete.

Port's databases are configured to perform a daily snapshot of the data. DB instance backups are retained for a limited period (i.e., a retention period) and are verified periodically. The backup system automatically generates a backup log, which is reviewed by the DevOps team to verify that the backup has been successfully completed. Failures, if any, are identified by a success/fail notification and resolved in the next day's backup cycle.

Port's Recovery Time Objective (RTO) is 12 hours, and its Recovery Point Objective (RPO) is 24 hours.

To protect data at rest, Port deploys industry-leading encryption algorithms to secure customer data, files, and media that reside in Port storage systems. All data is encrypted with advanced encryption standards. Access to database resources, which are located within the production environment, is restricted to authorized individuals. Port uses role-based access control to control access to database resources and API actions, especially actions that create, modify, or delete data resources and actions that perform common administrative tasks, such as backing up and restoring DB instances. Following the least-privilege principle when granting permission using Identity and Access Management (IAM) policies, Port controls the actions that users can perform on the database resource.

Port database is backed up according to the backup policy. The logs are backed up on a daily basis (**48**). The database is backed up in the form of snapshots. The snapshots are stored on the AWS Cloud Platform. The storage is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. It is also designed to sustain the concurrent loss of data in different facilities.

Restore

Port validates the backup process by performing a backup restore procedure known as the Data Recovery (DR) test. A restore process is performed and documented on an annual basis (**50**).

Incident Management Process

Port defines the term "incident" as any irregular or adverse event that occurs to any user data or personal data (including personal data breaches), or that involves the availability and integrity of the company's systems or network.

Examples of security incidents include:

- Loss or theft of data or equipment on which data is stored (e.g., laptops, mobile phones, etc.)
- Denial of Service
- Hacking attack
- Unauthorized use of Port's digital resources
- Policy or system failure (e.g., a policy that does not require multiple overlapping security measures—if backup security measures are absent, failure of a single protective system can leave data vulnerable)
- Human error or employee negligence (e.g., leaving a password list in a publicly accessible location, technical staff misconfiguring a security service or device, etc.)
- Attempted fraud involving electronic systems or physical (non-electronic) systems or functions
- Suspected impropriety by the user, service provider, or vendor

Monitoring systems are deployed 24/7 to detect anomalies and service disruptions. Service interruptions and maintenance notifications are sent to customers (**21**). Opening an incident ticket is done manually by one of Port's employees in cases of (a) breaches of system security, (b) availability, (c) confidentiality, and (d) customers-reported issues.

In the event of an outage or a service issue, a notification is sent to the customers. An incident management application is available to Port's employees in order to report breaches of the system's security, availability, and confidentiality. Customers report issues to their assigned account managers through the support application, email, or phone. Critical incidents are discussed in the risk assessment meetings. Service interruptions are communicated to customers through email notifications.

Security Incident Response Policy

Port has a security incident response management policy. Incidents trigger tickets and are tracked to resolution (**40**). Whenever a security incident of a physical or electronic nature is suspected or confirmed, all parties covered by this policy are expected to follow the appropriate procedures detailed in this policy. Appropriate compliance and legal personnel are informed of personal data breaches to assist in the response to, and communication of, security incidents internally and externally.

The response process consists of three phases:

1) **Identification**: The security incident is recognized, reported to the Security Response Team (SRT), and confirmed.
2) **Assessment:** The SRT analyzes the security incident and evaluates it for possible causes.
3) **Response:** The SRT responds to each security incident.

If any security incident also involves a personal data breach, then the company will also follow the steps that are applicable for such a breach (as detailed under "Personal Data Breach").

Risk Assessment

The process of risk assessment is a critical component of Port's internal control system. A comprehensive risk assessment that identifies and evaluates changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives is performed. As part of this process, threats to system security are identified, evaluated and the risk from these threats is formally assessed. The process is documented and maintained and all remediation activities must be approved by management (**16**).

Risk Assessment Meeting

Risks and threats are evaluated by key Port stakeholders during an annual meeting. Action items are documented within minutes of the meeting (**15**). Environmental, regulatory, and technological changes are monitored, their effects assessed, and their policies updated accordingly. Summarized protocol (MOM) is saved in a dedicated folder and sent by email to relevant managers. Decisions based on the meeting are assigned to resource, including a due date for execution, and managed through Port's Change Management application. The DPO communicates the need to promote a DPIA in cases where there is a potentially adverse effect with regard to individuals' privacy rights. In addition, Port assesses on an annual basis, the risks that vendors and business partners represent to the achievement of the company's objectives (**18**).

Risk Mitigation

Once the severity and likelihood of a potential risk have been assessed, management considers how the risk should be mitigated. The mitigation process involves making inferences based on assumptions about the risk and carrying out a cost-benefit analysis. Necessary actions are taken to reduce the level of severity, or the likelihood of the risk occurring and identify the control activities necessary to mitigate the risk. Port selects and develops control activities that contribute to risk mitigation, which achieves the company's acceptable objective levels. The risk mitigation process is integrated with the company's risk assessment. Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the Company's objectives during response, mitigation, and recovery efforts (**17**). In addition, Port has implemented a vendor management policy which details the vendor termination process. The policy is reviewed and approved annually (**19**).

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. The financial impacts of the risks are also taken into consideration during the process.

Confidentiality Procedures

Customer confidentiality is of great importance to Port As such, Port has implemented security measures to ensure the confidentiality of its customers' sensitive personal information (SPI). The security measures aim to prevent unauthorized access, disclosure, alteration, or destruction of sensitive personal information. Customer data has a single classification according to Port's information security policy. Upon customer request at the end of a contract agreement, Port will dispose of customer confidential information (**54**). Business partners are required to sign an agreement containing a confidentiality clause (**53**). Third-party infrastructure providers sign confidentiality agreements with Port in order to maintain system confidentiality, which conforms to Port's confidentiality policy.

Equipment contacting sensitive information is disposed of only after the sensitive information has been wiped out, including revocation of access permissions to the systems and premises as well as the return of company property and equipment. Customer data at rest is encrypted and hosted separately via secured storage services provided by AWS. Access to Port's DB resources, which are located within the production environment, is restricted to authorized personnel. The access to the production environment is performed using a two-factor authentication (**26**). Access to the production environment is restricted to authorized personnel based on job function and least privilege. Access to the AWS management interface is performed using MFA and is restricted to authorized personnel. Encryption between the company's customers and the application is enabled using an authenticated TLS tunnel. Additionally, the input and output of customer sessions and transactions are performed using a unique token that is assigned automatically. Finally, a risk assessment meeting is performed on a quarterly basis in order to evaluate risks and threats and to discuss and address security, confidentiality, and availability non-compliance issues. Minutes of the meetings are retained. In the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive, impacted customers are notified.

Subservice Organizations carved-out controls: Amazon Web Services (AWS)

The subservice organization is expected to:

- Implement controls to enable security and monitoring tools within the production environment
- Implement logical-access security measures for infrastructure components, including native security or security software and appropriate configuration settings
- Restrict access to virtual and physical servers, software, firewalls, and physical storage to authorized individuals
- Review the list of users and permissions on a regular basis
- Implement controls to:
  - Provide 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
- Allow only authorized tested and documented changes to be made to the system

Complementary User Entity Controls (CUECs)

In designing its system, Port allows for certain complementary controls to be implemented by user organizations to meet certain criteria applicable to security, availability, and confidentiality. A customer organization's overall internal control structure should be in operation and evaluated in conjunction with Port's controls presented in this section of the report.

The Kost Forer Gabbay and Kasierer (KFGK) examination was limited to the design of the controls in place at Port as they relate to Port's customers. Accordingly, the examination did not extend to any controls beyond those listed in this report or those in place at customer organizations. The Complementary User Entity Controls section describes controls that have to be placed in operation at customers to complement Port's controls. It is each interested party's responsibility to evaluate the user entity control considerations presented in this section in relation to the internal controls that are in place at customer organizations in order to obtain a complete understanding of the total internal control structure surrounding the Port Hosted Services and Application and to assess risk control. The portions of the internal control provided by the customer organizations are to be evaluated together with Port If effective customer organization internal controls are not in place, Port's controls may not be adequate to compensate for such weaknesses. Furthermore, this list is only a partial list of controls that customer organizations should have in place in order to complement the controls of Port.

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

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

Testing Performed and Results of Tests of Entity-Level Controls

In planning the nature, timing, and extent of its testing of the controls specified by Port, Kost Forer Gabbay & Kasierer (KFGK) considered aspects of Port ’s control environment, risk assessment processes, information and communication, and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

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

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

Criteria and Control

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by and are the responsibility of Port. The testing performed by KFGK and the results of the tests are the responsibility of the service auditor. Refer to the Trust Services criteria mapping section for the mapping of these controls to the Trust Services criteria.

Control Environment

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
7	Job descriptions are documented and maintained within the Port website and on external tools. Candidates go through screening and appropriate reference checks.	Inspected Port's website and determined that job descriptions were documented and maintained within the company website. Inspected the reference checks for a sample of new employees and determined that candidates went through screening and appropriate reference checks.	No deviations noted.
9	New employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses.	Inspected the signed employment agreement for a sample of new employees and determined the agreement included confidentiality and intellectual properly clauses.	No deviations noted.
53	Business partners are required to sign an agreement containing a confidentiality clause.	Inspected examples of signed business partner agreements and determined that the agreements contained a confidentiality clause.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda with (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda with (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The management of the company meets on at least a monthly basis to discuss on-going issues and updates.	Inspected a sample of management meeting minutes and invitations and determined that the management met on at least a monthly basis and that meeting minutes were retained.	No deviations noted.
3	An organizational chart is documented and approved by management that clearly defines management authorities and reporting hierarchy.	Inspected Port's organizational chart and determined that the chart was documented and management authorities and reporting hierarchy were clearly defined.	No deviations noted.
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to Port's employees within the Port internal portal.	Inspected the policies and determined that policies were documented, reviewed and approved by management on an annual basis. Inspected the internal portal and determined that policies were available to employees.	No deviations noted.
6	An information security policy is documented, reviewed and approved by Port management on an annual basis. The security policy is available to Port employees within the Port portal.	Inspected Port's Information Security policy and determined that the policy was documented, reviewed and approved by management on an annual basis. Inspected the internal portal and determined that the policy was available to employees within the Port portal.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
7	Job descriptions are documented and maintained within the Port website and on external tools. Candidates go through screening and appropriate reference checks.	Inspected Port's website and determined that job descriptions were documented and maintained within the company website. Inspected the reference checks for a sample of new employees and determined that candidates went through screening and appropriate reference checks.	No deviations noted.
8	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different Port policies and work procedures.	Inspected the onboarding checklists for a sample of new employees and determined that new employees went through an onboarding process during which, among others, were communicated their responsibilities and the different Port policies.	**Deviation noted:** Requested the evidence of the onboarding checklist for a sample of new employees. The company was unable to provide evidence of the onboarding checklist for one out of five employees in the requested sample. **Management's Response:** The new employee initially started as a contractor and transitioned to full-time during the audit period. To address this, Port has implemented an HR maintenance system to ensure proper documentation of the process in the future.
10	Employees go through annual security awareness training based on the Port security policy.	Inspected the security awareness training materials and the list of participants for a sample of employees and determined that employees went through awareness training on an annual basis.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
11	Personnel responsible for the design, development, implementation, and operation of systems affecting security, availability, confidentiality, undergo training on an ad-hoc basis.	Inspected Port's training program and the certification of completion for a sample of R&D employees and determined that training was performed on an ad-hoc basis by R&D personnel.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3	An organizational chart is documented and approved by management that clearly defines management authorities and reporting hierarchy.	Inspected Port's organizational chart and determined that the chart was documented and management authorities and reporting hierarchy were clearly defined.	No deviations noted.
8	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different Port policies and work procedures.	Inspected the onboarding checklists for a sample of new employees and determined that new employees went through an onboarding process during which, among others, were communicated their responsibilities and the different Port policies.	**Deviation noted:** Requested the evidence of the onboarding checklist for a sample of new employees. The company was unable to provide evidence of the onboarding checklist for one out of five employees in the requested sample. **Management's Response:** The new employee initially started as a contractor and transitioned to full-time during the audit period. To address this, Port has implemented an HR maintenance system to ensure proper documentation of the process in the future.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
9	New employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses.	Inspected the signed employment agreement for a sample of new employees and determined the agreement included confidentiality and intellectual properly clauses.	No deviations noted.
11	Personnel responsible for the design, development, implementation, and operation of systems affecting security, availability, confidentiality, undergo training on an ad-hoc basis.	Inspected Port's training program and the certification of completion for a sample of R&D employees and determined that training was performed on an ad-hoc basis by R&D personnel.	No deviations noted.

Communication and Information

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
15	Risks and threats are evaluated by key Port stakeholders during an annual meeting. Action items are documented within minutes of the meeting.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key Port stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were observed.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	A description of the Port system and its boundaries is documented and communicated to the relevant Port employees within the internal portal and to external users through Port's website.	Inspected Port's website and determined that a description of the Port system and its boundaries were documented and available to employees. Inspected Port's website and determined that a description of the Port system and its boundaries were documented and available to external users.	No deviations noted.
5	Policies and procedures are documented, reviewed and approved on an annual basis by the	Inspected the policies and determined that policies were documented, reviewed and approved by management on an annual basis.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	management team and available to Port's employees within the Port internal portal.	Inspected the internal portal and determined that policies were available to employees.	
6	An information security policy is documented, reviewed and approved by Port management on an annual basis. The security policy is available to Port employees within the Port portal.	Inspected Port's Information Security policy and determined that the policy was documented, reviewed and approved by management on an annual basis. Inspected the internal portal and determined that the policy was available to employees within the Port portal.	No deviations noted.
8	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different Port policies and work procedures.	Inspected the onboarding checklists for a sample of new employees and determined that new employees went through an onboarding process during which, among others, were communicated their responsibilities and the different Port policies.	**Deviation noted:** Requested the evidence of the onboarding checklist for a sample of new employees. The company was unable to provide evidence of the onboarding checklist for one out of five employees in the requested sample. **Management's Response:** The new employee initially started as a contractor and transitioned to full-time during the audit period. To address this, Port has implemented an HR maintenance system to ensure proper documentation of the process in the future.
10	Employees go through annual security awareness training based on the Port security policy.	Inspected the security awareness training materials and the list of participants for a sample of employees and determined that employees went through awareness training on an annual basis.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
22	Uptime requirements are defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.	Inspected the internal company SLA agreement and determined that uptime requirements were defined in the company's SLA.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	A description of the Port system and its boundaries is documented and communicated to the relevant Port employees within the internal portal and to external users through Port's website.	Inspected Port's website and determined that a description of the Port system and its boundaries were documented and available to employees. Inspected Port's website and determined that a description of the Port system and its boundaries were documented and available to external users.	No deviations noted.
12	New features are communicated to customers, if relevant, through emails, the website or directly through the account manager.	Inspected a sample of release notes and determined that new features were communicated to customers through emails, the website or directly through the account manager.	No deviations noted.
21	Service interruptions and maintenance notifications are sent to customers.	Inspected the Port's status page and determined that the uptime report was available to customers.	No deviations noted.
22	Uptime requirements are defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.	Inspected the internal company SLA agreement and determined that uptime requirements were defined in the company's SLA.	No deviations noted.

Risk Assessment

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
15	Risks and threats are evaluated by key Port stakeholders during an annual meeting. Action items are documented within minutes of the meeting.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key Port stakeholders during an annual risk	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		assessment. Minutes of risk assessment meetings and actions items were observed.	
16	A comprehensive risk assessment that identifies and evaluates changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives is performed. As part of this process, threats to system security are identified, evaluated and the risk from these threats is formally assessed. The process is documented and maintained and all remediation activities must be approved by management.	Inspected the risk assessment documentation and determined that it was performed and documented annually.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda with (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The management of the company meets on at least a monthly basis to discuss on-going issues and updates.	Inspected a sample of management meeting minutes and invitations and determined that the management met on at least a monthly basis and that meeting minutes were retained.	No deviations noted.
15	Risks and threats are evaluated by key Port stakeholders during an annual meeting. Action items are documented within minutes of the meeting.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key Port stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were observed.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
16	A comprehensive risk assessment that identifies and evaluates changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives is performed. As part of this process, threats to system security are identified, evaluated and the risk from these threats is formally assessed. The process is documented and maintained and all remediation activities must be approved by management.	Inspected the risk assessment documentation and determined that it was performed and documented annually.	No deviations noted.
37	Vulnerability scans are performed continuously using the source code tool as a part of the SDLC process.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously on source code.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda with (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The management of the company meets on at least a monthly basis to discuss on-going issues and updates.	Inspected a sample of management meeting minutes and invitations and determined that the management met on at least a monthly basis and that meeting minutes were retained.	No deviations noted.
15	Risks and threats are evaluated by key Port stakeholders during an annual meeting. Action items are documented within minutes of the meeting.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key Port stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were observed.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
16	A comprehensive risk assessment that identifies and evaluates changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives is performed. As part of this process, threats to system security are identified, evaluated and the risk from these threats is formally assessed. The process is documented and maintained and all remediation activities must be approved by management.	Inspected the risk assessment documentation and determined that it was performed and documented annually.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda with (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The management of the company meets on at least a monthly basis to discuss on-going issues and updates.	Inspected a sample of management meeting minutes and invitations and determined that the management met on at least a monthly basis and that meeting minutes were retained.	No deviations noted.
37	Vulnerability scans are performed continuously using the source code tool as a part of the SDLC process.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously on source code.	No deviations noted.
38	An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved.	Inspected the penetration test report and determined that it was performed on an annual basis.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the penetration test report and determined that critical and high issues were investigated and resolved.	

Monitoring Activities

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
18	Port assesses on an annual basis, the risks that vendors and business partners represent to the achievement of the company's objectives.	Inspected the vendor assessment and determined that vendors were assessed annually for the risk they may represent to the achievement of the company's objectives.	No deviations noted.
23	Actions performed on the production environment, including OS, DB and application are monitored, logged and reviewed. Alerts are triggered upon the identification of an anomaly.	Inspected the monitoring logs and determined that actions performed on the production and database environments were logged and reviewed. Inspected a sample of alerts and determined that alerts were triggered upon the identification of an anomaly.	No deviations noted.
24	Port uses a suite of monitoring tools in order to monitor its service. The production environment, including the servers and application, is monitored by the Operation Team. Key Port personnel are notified of events related to the security, availability, or confidentiality of service to clients.	Inspected Port’s monitoring dashboards and configuration and determined that Port used a suite of monitoring tools to monitor its service and that alerts were sent to relevant stakeholders by an internal communication tool, based on pre-defined rules. Inspected Port’s monitoring dashboards and configuration and determined that Port used a suite of monitoring tools to monitor its service.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda with (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The management of the company meets on at least a monthly basis to discuss on-going issues and updates.	Inspected a sample of management meeting minutes and invitations and determined that the management met on at least a monthly basis and that meeting minutes were retained.	No deviations noted.
24	Port uses a suite of monitoring tools in order to monitor its service. The production environment, including the servers and application, is monitored by the Operation Team. Key Port personnel are notified of events related to the security, availability, or confidentiality of service to clients.	Inspected Port's monitoring dashboards and configuration and determined that Port used a suite of monitoring tools to monitor its service and that alerts were sent to relevant stakeholders by an internal communication tool, based on pre-defined rules. Inspected Port's monitoring dashboards and configuration and determined that Port used a suite of monitoring tools to monitor its service.	No deviations noted.

Control Activities

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
15	Risks and threats are evaluated by key Port stakeholders during an annual meeting. Action items are documented within minutes of the meeting.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key Port stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were observed.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to Port's employees within the Port internal portal.	Inspected the policies and determined that policies were documented, reviewed and approved by management on an annual basis. Inspected the internal portal and determined that policies were available to employees.	No deviations noted.
10	Employees go through annual security awareness training based on the Port security policy.	Inspected the security awareness training materials and the list of participants for a sample of employees and determined that employees went through awareness training on an annual basis.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3	An organizational chart is documented and approved by management that clearly defines management authorities and reporting hierarchy.	Inspected Port's organizational chart and determined that the chart was documented and management authorities and reporting hierarchy were clearly defined.	No deviations noted.
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to Port's employees within the Port internal portal.	Inspected the policies and determined that policies were documented, reviewed and approved by management on an annual basis. Inspected the internal portal and determined that policies were available to employees.	No deviations noted.
6	An information security policy is documented, reviewed and approved by Port management on an annual basis. The security policy is available to Port employees within the Port portal.	Inspected Port's Information Security policy and determined that the policy was documented, reviewed and approved by management on an annual basis. Inspected the internal portal and determined that the policy was available to employees within the Port portal.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
19	Port has implemented a vendor management policy which details the vendor termination process. The policy is reviewed and approved annually.	Inspected the vendor management policy and determined that the policy was documented, reviewed, and approved annually. Inspected the vendor management policy and determined that Port detailed the vendor termination process.	No deviations noted.
22	Uptime requirements are defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.	Inspected the internal company SLA agreement and determined that uptime requirements were defined in the company's SLA.	No deviations noted.
41	There is a documented change management policy. The policy is reviewed and approved on an annual basis.	Inspected the change management policy and determined that the policy was reviewed and approved on an annual basis.	No deviations noted.

Logical and Physical Access Controls

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
25	Users are identified through the use of a user ID/password combination using an SSO tool. Strong password configuration settings, where applicable, are enabled including: (1) forced password change at defined intervals, (2) a minimum password length, (3) a limit on the number of tempts to enter a password before the user ID is suspended, and (4) password complexity.	Inspected the Single Sign-On password configuration settings and determined that strong password configuration settings, where applicable, were enabled on the SSO and native tools including: (1) forced password change at defined intervals, (2) a minimum password length, (3) a limit on the number of tempts to enter a password before the user ID was suspended, and (4) password complexity.	No deviations noted.
26	The access to the production environment is performed using a two-factor authentication.	Inspected the list of users with access to the production environment and determined it was restricted to authorized personnel.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the production environment access configuration and determined that two-factor authentication was enabled.	
27	The access to the deployment tool required MFA and is restricted to authorized personnel.	Inspected the list of users with access to the deployment tool and determined it was restricted to authorized personnel. Inspected the deployment tool access configuration and determined that MFA was enabled.	No deviations noted.
29	Developers do not have access to the production and database environments. Specific developers can be granted access for specific projects. These accesses are logged and reviewed.	Inspected the list of users with access permissions to the production and database environment and determined that developers did not have access to the production. Inspected the log configuration and determined that accesses were logged and reviewed.	No deviations noted.
31	Access to the source control tool is performed using MFA and is restricted to authorized personnel.	Inspected the list of users with access to the source control tool and determined it was restricted to authorized personnel. Inspected the list of users with access to the source control tool and determined that MFA was enabled.	No deviations noted.
45	The permission to approve merge requests and to deploy is restricted to authorized personnel.	Inspected the list of users with permission to approve merge requests and to deploy and determined that it was restricted to authorized personnel.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
28	Terminated employees who had access to the production environment have their permissions removed and company equipment returned in a timely manner.	Inspected the offboarding checklist for a sample of terminated employees and determined that permissions were revoked in a timely manner and assets were returned.	No deviations noted.
32	New employees are granted access to the different environments by a ticketing system process and subject to manager approval.	Inspected documentation for a sample of new employees and determined that granting of new access was triggered as part of the onboarding process.	**Deviation noted:** Requested the evidence of the onboarding checklist for a sample of new employees. The company was unable to provide evidence of the onboarding checklist for one out of five employees in the requested sample. **Management's Response:** The new employee initially started as a contractor and transitioned to full-time during the audit period. To address this, Port has implemented an HR maintenance system to ensure proper documentation of the process in the future.
33	Permissions to the different environments (production, databases and applications) are reviewed, approved and documented by the Port.io management on an annual basis.	Inspected the user access review documentation and determined that accesses and permissions for the different environments were reviewed and approved by the management on an annual basis.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
28	Terminated employees who had access to the production environment have their permissions removed and company equipment returned in a timely manner.	Inspected the offboarding checklist for a sample of terminated employees and determined that permissions were revoked in a timely manner and assets were returned.	No deviations noted.
32	New employees are granted access to the different environments by a ticketing system process and subject to manager approval.	Inspected documentation for a sample of new employees and determined that granting of new access was triggered as part of the onboarding process.	**Deviation noted:** Requested the evidence of the onboarding checklist for a sample of new employees. The company was unable to provide evidence of the onboarding checklist for one out of five employees in the requested sample. **Management's Response:** The new employee initially started as a contractor and transitioned to full-time during the audit period. To address this, Port has implemented an HR maintenance system to ensure proper documentation of the process in the future.
33	Permissions to the different environments (production, databases and applications) are reviewed, approved and documented by the Port.io management on an annual basis.	Inspected the user access review documentation and determined that accesses and permissions for the different environments were reviewed and approved by the management on an annual basis.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
34	Physical access to the offices is restricted to authorized personnel using a personal identification card according to the physical access policy.	Inspected the physical access policy and determined that physical access was restricted to authorized personnel using personal identification cards.	No deviations noted.
35	Visitors to the Port office are accompanied while on premises.	Inspected the physical access policy and determined that visitors were accompanied while on premises.	No deviations noted.
36	Port.io performs a review of the SOC 2 report of its third party infrastructure provider on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at Port.io to address the CUECs.	Inspected the review of the data center SOC 2 report performed by Port and determined that the review was performed annually and included investigation of deviations and identifying and documenting the controls in place at Port to address the CUECs.	No deviations noted.

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

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

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
30	Access to system resources is protected through a combination of firewalls, VPNs, native operating system security, database management system security, application controls and intrusion detection monitoring software.	Inspected the system architecture diagram and determined that access was protected through a combination of firewalls, VPNs, native operating system security, database management system security and application controls.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
52	Interactions between customers and the Port platform are performed by using an encrypted channel based on an authenticated SSL connection.	Inspected the encryption configuration and determined that the encryption between Port customers and the Port application was enabled using an authenticated SSL tunnel.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
30	Access to system resources is protected through a combination of firewalls, VPNs, native operating system security, database management system security, application controls and intrusion detection monitoring software.	Inspected the system architecture diagram and determined that access was protected through a combination of firewalls, VPNs, native operating system security, database management system security and application controls.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
37	Vulnerability scans are performed continuously using the source code tool as a part of the SDLC process.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously on source code.	No deviations noted.
38	An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved.	Inspected the penetration test report and determined that it was performed on an annual basis. Inspected the penetration test report and determined that critical and high issues were investigated and resolved.	No deviations noted.
39	Antivirus software is installed on workstations and laptops supporting such software. Port uses a centralized management tool in order to receive alerts of the antivirus status.	Inspected a sample of employees' laptops and dashboards and determined that an antivirus solution was installed on employees' laptops.	No deviations noted.

System Operations

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
37	Vulnerability scans are performed continuously using the source code tool as a part of the SDLC process.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously on source code.	No deviations noted.
38	An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved.	Inspected the penetration test report and determined that it was performed on an annual basis. Inspected the penetration test report and determined that critical and high issues were investigated and resolved.	No deviations noted.
39	Antivirus software is installed on workstations and laptops supporting such software. Port uses a centralized management tool in order to receive alerts of the antivirus status.	Inspected a sample of employees' laptops and dashboards and determined that an antivirus solution was installed on employees' laptops.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
22	Uptime requirements are defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.	Inspected the internal company SLA agreement and determined that uptime requirements were defined in the company's SLA.	No deviations noted.
24	Port uses a suite of monitoring tools in order to monitor its service. The production environment, including the servers and application, is monitored by the Operation Team. Key Port personnel are notified of events related to the security, availability, or confidentiality of service to clients.	Inspected Port's monitoring dashboards and configuration and determined that Port used a suite of monitoring tools to monitor its service and that alerts were sent to relevant stakeholders by an internal communication tool, based on pre-defined rules.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected Port's monitoring dashboards and configuration and determined that Port used a suite of monitoring tools to monitor its service.	
38	An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved.	Inspected the penetration test report and determined that it was performed on an annual basis. Inspected the penetration test report and determined that critical and high issues were investigated and resolved.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
24	Port uses a suite of monitoring tools in order to monitor its service. The production environment, including the servers and application, is monitored by the Operation Team. Key Port personnel are notified of events related to the security, availability, or confidentiality of service to clients.	Inspected Port's monitoring dashboards and configuration and determined that Port used a suite of monitoring tools to monitor its service and that alerts were sent to relevant stakeholders by an internal communication tool, based on pre-defined rules. Inspected Port's monitoring dashboards and configuration and determined that Port used a suite of monitoring tools to monitor its service.	No deviations noted.
37	Vulnerability scans are performed continuously using the source code tool as a part of the SDLC process.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously on source code.	No deviations noted.
40	Port has a security incident response management policy. Incidents trigger tickets and are tracked to resolution.	Inspected the incident response policy and determined that it defined the steps to be taken upon identification of a security incident. During the audit period, no security events occurred.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
37	Vulnerability scans are performed continuously using the source code tool as a part of the SDLC process.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously on source code.	No deviations noted.
40	Port has a security incident response management policy. Incidents trigger tickets and are tracked to resolution.	Inspected the incident response policy and determined that it defined the steps to be taken upon identification of a security incident. During the audit period, no security events occurred.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
21	Service interruptions and maintenance notifications are sent to customers.	Inspected the Port's status page and determined that the uptime report was available to customers.	No deviations noted.
37	Vulnerability scans are performed continuously using the source code tool as a part of the SDLC process.	Inspected the vulnerability scanning configuration and determined that vulnerability scans were configured to run continuously on source code.	No deviations noted.
40	Port has a security incident response management policy. Incidents trigger tickets and are tracked to resolution.	Inspected the incident response policy and determined that it defined the steps to be taken upon identification of a security incident. During the audit period, no security events occurred.	No deviations noted.
50	A restore process is performed and documented on an annual basis.	Inspected the restoration test results and determined that the restore process was performed successfully and documented on an annual basis.	No deviations noted.

Change Management

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
41	There is a documented change management policy. The policy is reviewed and approved on an annual basis.	Inspected the change management policy and determined that the policy was reviewed and approved on an annual basis.	No deviations noted.
42	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved within the change management application.	Inspected the change management tickets for a sample of commits that were merged in the production and determined that changes were documented and labeled based on the development phase and urgency. Inspected the change management tickets for a sample of commits that were merged in the production and determined that tickets contained a documented description of the required change.	No deviations noted.
43	Tickets in the change management tool are connected to the source control tool in order to link the request to the code change.	Inspected the change management tickets for a sample of commits that were merged in the production and determined that tickets were linked to the actual code in the version control tool.	No deviations noted.
44	Code changes are reviewed along with the pull request performed by the team leader. The code review is documented on the source control tool. Code review is mandatory in order to continue in the SDLC process and deploy a version to the production environment.	Inspected the pull requests for a sample of commits that were merged in the production and determined that code review took place as part of the change management approval process. Inspected the source control tool configuration and determined that code review was mandatory to continue in the SDLC process.	No deviations noted.
46	Automation tests are performed using a dedicated tool on a regular basis in order to identify issues within the application.	Inspected a sample of commits that were merged in the production and determined that changes went through automated testing.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
47	A successful test status is required to continue in the SDLC process.	Inspected the source control tool's configuration and determined that a successful test status was mandatory in order to continue with the SDLC process.	No deviations noted.

Risk Mitigation

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
9	New employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses.	Inspected the signed employment agreement for a sample of new employees and determined the agreement included confidentiality and intellectual properly clauses.	No deviations noted.
15	Risks and threats are evaluated by key Port stakeholders during an annual meeting. Action items are documented within minutes of the meeting.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key Port stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were observed.	No deviations noted.
17	Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the Company's objectives during response, mitigation, and recovery efforts.	Inspected the risk assessment documentation and determined that a mitigation plan was associated with each identified risk.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	The management of the company meets on at least a monthly basis to discuss on-going issues and updates.	Inspected a sample of management meeting minutes and invitations and determined that the management met on at least a monthly basis and that meeting minutes were retained.	No deviations noted.
18	Port assesses on an annual basis, the risks that vendors and business partners represent to the achievement of the company's objectives.	Inspected the vendor assessment and determined that vendors were assessed annually for the risk they may represent to the achievement of the company's objectives.	No deviations noted.
19	Port has implemented a vendor management policy which details the vendor termination process. The policy is reviewed and approved annually.	Inspected the vendor management policy and determined that the policy was documented, reviewed, and approved annually. Inspected the vendor management policy and determined that Port detailed the vendor termination process.	No deviations noted.
34	Physical access to the offices is restricted to authorized personnel using a personal identification card according to the physical access policy.	Inspected the physical access policy and determined that physical access was restricted to authorized personnel using personal identification cards.	No deviations noted.
35	Visitors to the Port office are accompanied while on premises.	Inspected the physical access policy and determined that visitors were accompanied while on premises.	No deviations noted.
36	Port.io performs a review of the SOC 2 report of its third party infrastructure provider on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at Port.io to address the CUECs.	Inspected the review of the data center SOC 2 report performed by Port and determined that the review was performed annually and included investigation of deviations and identifying and documenting the controls in place at Port to address the CUECs.	No deviations noted.
53	Business partners are required to sign an agreement containing a confidentiality clause.	Inspected examples of signed business partner agreements and determined that the agreements contained a confidentiality clause.	No deviations noted.

Availability

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
24	Port uses a suite of monitoring tools in order to monitor its service. The production environment, including the servers and application, is monitored by the Operation Team. Key Port personnel are notified of events related to the security, availability, or confidentiality of service to clients.	Inspected Port’s monitoring dashboards and configuration and determined that Port used a suite of monitoring tools to monitor its service and that alerts were sent to relevant stakeholders by an internal communication tool, based on pre-defined rules. Inspected Port’s monitoring dashboards and configuration and determined that Port used a suite of monitoring tools to monitor its service.	No deviations noted.
49	Port databases are replicated in several availability zones.	Inspected the Port database's configuration and determined that it was replicated in several availability zones.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
21	Service interruptions and maintenance notifications are sent to customers.	Inspected the Port's status page and determined that the uptime report was available to customers.	No deviations noted.
48	Port database is backed up according to the backup policy. The logs are backed up on a daily basis.	Inspected the database backup configuration and determined that the Port application database was backed up on a daily basis.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
50	A restore process is performed and documented on an annual basis.	Inspected the restoration test results and determined that the restore process was performed successfully and documented on an annual basis.	No deviations noted.

Confidentiality

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda with (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The management of the company meets on at least a monthly basis to discuss on-going issues and updates.	Inspected a sample of management meeting minutes and invitations and determined that the management met on at least a monthly basis and that meeting minutes were retained.	No deviations noted.
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to Port's employees within the Port internal portal.	Inspected the policies and determined that policies were documented, reviewed and approved by management on an annual basis. Inspected the internal portal and determined that policies were available to employees.	No deviations noted.
9	New employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses.	Inspected the signed employment agreement for a sample of new employees and determined the agreement included confidentiality and intellectual properly clauses.	No deviations noted.
51	Customer passwords are encrypted within the database.	Inspected the external tool configuration and determined that customer passwords were encrypted according to the Port security policy.	No deviations noted.
53	Business partners are required to sign an agreement containing a confidentiality clause.	Inspected examples of signed business partner agreements and determined that the agreements contained a confidentiality clause.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
54	Upon customer request at the end of a contract agreement, Port will dispose of customer confidential information.	Inspected the service termination procedure and determined that it outlined the steps to undertake if a client requested to have their confidential information disposed of. During the audit period, no such events occurred.	No deviations noted.

****