SOC 2 Type I Report

As of May 26, 2024

REPORT ON CONTROLS PLACED IN OPERATION AT CYBORD RELEVANT TO SECURITY AND CONFIDENTIALITY
WITH THE INDEPENDENT SERVICE AUDITOR'S REPORT

Table of Contents

Cybord

Section I – Cybord Ltd.'s Management Assertion

June 30, 2024

We have prepared the accompanying "Description of the Cybord Platform relevant to Security and Confidentiality as of May 26, 2024" (Description) of Cybord 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 Cybord Platform (System) that may be useful when assessing the risks from interactions with the System, particularly information about system controls that Cybord Ltd. has designed, implemented, and operated as of May 26, 2024 to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteri*a.

Carved-out Unaffiliated Subservice Organization: Cybord Ltd. uses Amazon Web Services ('AWS') to provide infrastructure management services. The Description includes only the controls Cybord Ltd. and excludes controls of AWS. The Description indicates that complementary controls at AWS that are suitably designed and operating effectively are necessary, along with controls at Cybord Ltd. to achieve the service commitments and system requirements. The Description presents Cybord Ltd.'s controls and the types of complementary subservice organization controls assumed in the design of Cybord 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 as of May 26, 2024, in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed as of May 26, 2024 to provide reasonable assurance that the Cybord 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 Cybord Ltd.'s controls.

Shir Caplan, VP of R&D

Oshri Cohen, CEO

[**Signature**]
Title

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

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

Section II – Independent service auditor's report

To the Management of Cybord Ltd.

Scope

We have examined Cybord Ltd.'s accompanying "Description of the Cybord Platform relevant to Security and Confidentiality as of May 26, 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 (With Revised Implementation Guidance — 2022)* (Description Criteria) and the suitability of the design of controls stated in the Description as of May 26, 2024 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*, in AICPA Trust Services Criteria.

Cybord 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 Cybord Ltd., to provide reasonable assurance that Cybord Ltd.'s service commitments and system requirements are achieved based on the applicable trust services criteria. The description presents Cybord 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 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 as of May 26, 2024.

Cybord Ltd.'s responsibilities

Cybord 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. Cybord Ltd. has provided the accompanying assertion titled, Management Assertion of Cybord Ltd. (Assertion) about the presentation of the Description based on the Description Criteria and the suitability of design 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. Cybord 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 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 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 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria as of May 26, 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 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 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.
- evaluating the overall presentation of the Description.

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

We are required to be independent of Cybord 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.

Other matter

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

Opinion

In our opinion, in all material respects:

a. the Description presents the Cybord Platform system that was designed and implemented as of May 26, 2024 in accordance with the Description Criteria.

b. the controls stated in the Description were suitably designed as of May 26, 2024 to provide reasonable assurance that Cybord Ltd.'s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively as of May 26, 2024 and if the subservice organization and user entities applied the complementary controls assumed in the design of Cybord Ltd.'s controls as of May 26, 2024.

Restricted use

This report is intended solely for the information and use of Cybord Ltd., user entities of Cybord Ltd.'s system as of May 26, 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 organization, or other parties.
- Internal control and its limitations.
- 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
A member firm of Ernst & Young Global

June 30, 2024
Tel-Aviv, Israel

Cybord

Section III – Description of the Cybord Platform Service relevant to Security and Confidentiality as of May 26, 2024

Company Overview and Background

Cybord was founded by Dr. Eyal Weiss, Cybord has taken on a mission to get counterfeit and defective components off production lines. The Cybord Deep Visual-AI platform aggregates and analyzes images and data from 100% of the electronic components. It combines existing production data and new visual data collection, and ensures product quality, authenticity, and traceability, for OEMs and EMSs.

Purpose and Scope of the Report

The scope of this report is limited to the controls supporting the Cybord Platform and products and does not extend to other available software products and services or the controls at third 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*

Products and Services

Cybord QCI:

Ensures high yields of a product from its early assembly stages.

The Cybord QCI uses the images generated from the pick and place system, which are taken from the bottom of the component, and analyzes the parameters of the images captured by the SMT machines. The AI engine authenticates each assembled component and inspects quality and traceability attributes, to enforce components quality and ensure high productivity.

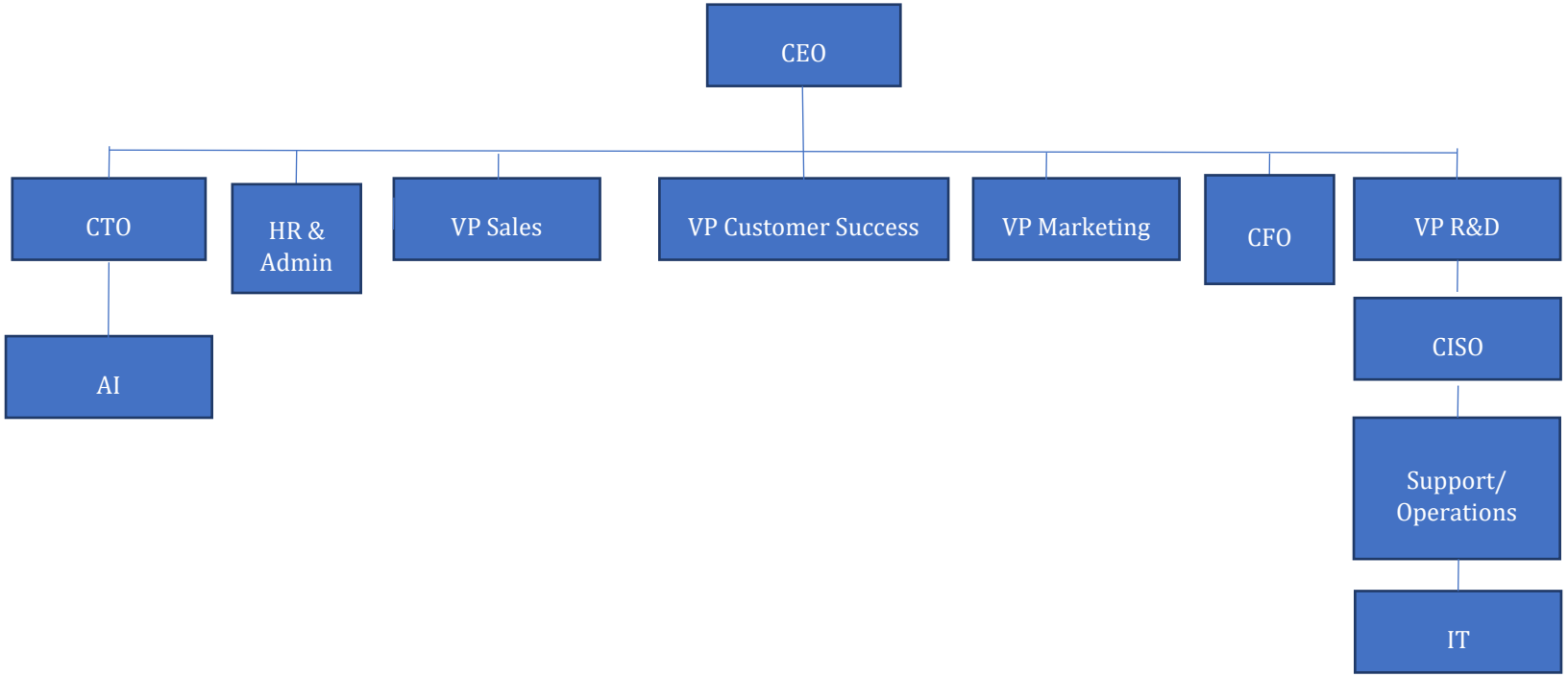
Cybord TCI:

Verifies the visual traceability of marked components assembled on each PCBA.

The Cybord TCI on the AOI (Automatic Optical Inspection) equipment verified all images taken from the top of the assembled PCBA. All component markings of images captured by AOI machines are decoded and cross-checked with traceability documentation, to detect and alert deviations from documented lot numbers and date codes.

Organizational Structure

Cybord's organizational structure provides the overall framework for planning, directing and controlling operations. It utilizes an approach whereby personnel and business functions are segregated into departments according to job responsibilities, lines of reporting and communications, and allows employees to focus on the specific business issues impacting their customers. An organizational chart is documented and approved by management that clearly defines management authorities and reporting hierarchy **(3).** Below is a description of key Cybord departments:



Sales:
The Sales department identifies, builds, and manages partnerships with third-party vendors to expand Cybord's offerings and customer base.

Marketing:
The Marketing department builds Cybord's brand awareness, generates qualified sales leads, and drives secure customer acquisition through marketing activities.

Customer Support:
The Customer Support team provides exceptional technical support to Cybord's customers, ensuring a secure and positive user experience.

Customer Success:
The Customer Success team analyzes market needs and incorporates client feedback into product roadmaps, guaranteeing Cybord's offerings meet evolving security and compliance requirements.

Research & Development (R&D):
R&D develops, tests, and validates secure Cybord products and business services implemented within the production environment.

AI
The AI department spearheads the development and integration of cutting-edge artificial intelligence solutions within the company's product offerings. This team works closely with R&D sub-teams to leverage AI.

Finance:
The Finance department manages Cybord's financial activities, including financial reporting, budgeting, and internal controls.

Overview of Company's Internal Control

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

Control Environment

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

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

(4) Organizational policies and procedures.

Board of Directors - The Board of Directors (BOD) of Cybord is comprised 5 directors of which 3 are appointed by Insight Partners. The company founder, who also serves as the CTO, and the CEO are also executive officers of the company. The Board of Directors is actively engaged in the governance of the Company and its strategic direction. 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. Meeting minutes are retained **(1).** The Board's responsibilities include but are not limited to (1) monitoring the actual performance of the Company through its financial results; (2) monitoring the Company's compliance with legal and regulatory requirements; (3) analysis of the budget vs actual results; (4) guiding the Company in the way it funds its operation; (5) approving arrangements with executive officers relating to their employment relationships with the Company, including, without limitation, employment agreements, severance agreements, change in control agreements and restrictive covenants and (6) approving equity-based compensation plans in which directors, officers or employees may participate.

Management Philosophy and Operating Style: The Management Team, chaired by the Chief Executive Officer ("CEO"), has been delegated by the Board the responsibility to manage Cybord and its business daily. Cybord is led by a team with proven ability in cyber security and code security customer solutions to the global market. In its role, the Management Team assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. The Management Team designs policies and communications so that personnel understand Cybord'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 a weekly basis to discuss on-going issues and updates. Meeting minutes are retained **(2).** In addition, the management team convenes off-site on a half-year basis for strategic purposes.

Integrity and Ethical values – Integrity and ethical values are essential elements of the control environment, affecting the design, administration and monitoring of key processes. Integrity and ethical behavior are the products of Cybord's ethical and behavioral standards, how they are communicated and how they are monitored and enforced in its business activities. They include management's actions to remove or reduce inappropriate incentives or extraneous pressures, and opportunities that might prompt personnel to engage in dishonest, illegal or unethical acts. They also include the communication of the organization's values and behavioral standards to personnel through policy statements and from the executives. The Board of Directors and Management Team recognize their responsibility to foster a strong ethical environment within Cybord to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct. Moreover, new employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses **(9).**

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

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

procedures **(8).** New professional employees that join Cybord are required to attend an On-Boarding welcome session (held every 3 months) which provides them with the necessary knowledge about the firm and general work procedures. In addition, Job descriptions are documented and maintained within the Cybord website. Candidates go through screening and appropriate reference checks **(7).** Also, employees go through a feedback process on at least an annual basis. The feedback reports are retained with the employee personal record **(14).**

Personnel responsible for the design, development, implementation, and operation of systems affecting security, availability, confidentiality, undergo training on an ad-hoc basis **(11).** Cybord's Team Leaders are responsible for training plans for their newcomers. Professional training for existing employees is typically done only for new tools. It is the manager's role to decide what training a particular employee requires as they relate to specific job requirements. An annual review for all employees takes place. Main review topics are Job perception, performance feedback, and manager-employee open discussion. Currently this review is not based on quantitative objectives. The review is written and submitted in native language (per site). Salary increases depend on promotion as well as evaluation discussions.

Control Activities

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

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

Risk Assessment

Risk identification: The process of identifying, assessing and managing risks is a critical component of Cybord's internal control system. The purpose of Cybord's risk assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives. Risk analysis embodies identification of key business processes in which potential exposures of some consequence exist. Exposures defined by Cybord, considers both internal and external influences that may harm the entity's ability to provide reliable services. It includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets. It also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and service, business partners, customers, and others with access to the Cybord's information systems. Also, risks and threats are evaluated by key Cybord stakeholders during an annual meeting. Action items are documented within minutes of the meeting **(16).**
Risk assessment: 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 **(17).** Also, Cybord assesses on an annual basis, the risks that vendors and business partners represent to the achievement of the company's objectives **(19).** Ongoing monitoring and risks assessment procedures are built into the normal recurring activities of Cybord and include regular management and supervisory activities. Identified risks are analyzed through a process that includes estimating their potential significance. The assessment

includes how the risk should be managed and whether to accept, avoid, reduce, or share the risk. Each department's managers are regularly in touch with personnel and may question the accuracy of information that differs significantly from their operations knowledge. The Management Team considers the significance of the identified risks by determining the criticality and impact of the risks.

Risk Mitigation: Once the severity and likelihood of a potential risk has been assessed, management considers how the risk should be mitigated. The mitigation process involves making inferences based on assumptions about the risk and carrying out a cost-benefit analysis. Necessary actions are taken to reduce the level of severity or the likelihood of the risk occurring, and the control activities necessary to mitigate the risk are identified. Cybord selects and develops control activities that contribute to the mitigation of risks to the achievement of the company's objectives to acceptable levels. The risk mitigation process is integrated with the company's risk assessment. Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the Company's objectives during response, mitigation, and recovery efforts **(18).**

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

Fraud assessment: The assessment of fraud considers:

- Fraudulent reporting.
- Possible loss of assets.
- Incentives and pressures.
- Corruption resulting from the various ways that fraud and misconduct can occur.
- How management and other personnel might engage in or justify inappropriate actions.
  Controls are in place at Cybord to evaluate and monitor the risks of fraud.

Information and Communication

Information and communication are an integral component of Cybord's internal control system. It is the process of identifying, capturing and exchanging information in the form and timeframe necessary to conduct, manage and control the organization's operations. At Cybord, information is identified, captured, processed and reported by various information systems, and through conversations with clients, vendors, regulators and employees.
Weekly management meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls and other strategic initiatives. Senior executives who lead the meetings use information gathered from formal automated information systems and informal databases, and conversations with various internal and external colleagues. General updates to organization-wide security policies and procedures are usually communicated to the appropriate Cybord personnel via email messages and shared with appropriate audiences through the internal communication tool. Availability, confidentiality and security related obligations are communicated to Cybord's employees through the confidentiality and non-disclosure agreements while client obligations and commitments are communicated within the contracts. In addition, Cybord's approved policies as well as the process of informing the entity about breaches of the system Security, Availability and Confidentiality are communicated to personnel responsible for implementing them in the internal application. In addition, a description of the Cybord system and its boundaries is documented and communicated to Cybord employees and to external users through the website

(4). Also, new features are communicated to customers, if relevant, through emails or dedicated meetings **(12).** And new features are communicated to employees through the internal portal **(13).**

General Company Policies

Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to Cybord's employees within the Cybord shared folders **(5).** Formal written policies for the principles and processes within the organization are developed and communicated so that personnel understand Cybord's objectives. The assigned policy owner updates the policy annually and the policy is reviewed and approved by designated members of management. In addition, Responsibility and accountability for developing and maintaining the policies are assigned to the Cybord relevant teams and are reviewed and approved on an annual basis by the management team.

Monitoring

Managers at Cybord are responsible for monitoring the quality and effectiveness of the various operations and internal controls as a routine part of their activities. Performance reports and statistics are generated regularly and presented to Executive management for evaluation. Management uses automated reports created through various applications and processes to monitor the efficiency of specific processes and the effectiveness of specific key controls. Metrics produced from these systems are used to identify the strengths and achievements, as well as the weaknesses, inefficiencies or potential performance issues with respect to a specific process. Managers have responsibility for informing their direct reports about these items at the appropriate time. The Executive Management Team monitors the progress with respect to Cybord service processes regularly. Root cause analysis is performed following security incidents **(45).** Analysis of root cause is performed through various tools and meetings, and corrective measures are communicated to relevant groups through e-mails, meetings, and a project portal tool to prevent future occurrences.

Asset Management

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

Logical and Physical Access

Cybord has established an organization-wide information security policy designed to protect information at a level commensurate with its value. The policy dictates security controls for media where information is stored, the systems that process it, as well as infrastructure components that facilitate its transmission. An information security policy is documented, reviewed and approved by Cybord management on an annual basis. The security policy is available to Cybord employees within the shared folders **(6).**

Access Control, User and Permissions Management

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

Cybord manages and delivers its services using a variety of systems and environments. As previously described, information security controls and procedures are implemented throughout these systems, to help prevent unauthorized

access to data. Authorized access to the AWS' hosting environment is performed directly from the Cybord office or using VPN to Cybord office then to servers' farm by using SAML authentication and two factors authentication. The database servers reside within the production environment. The access to the production environment servers is restricted to authorized personnel (refer to section 'Production Environment Logical Access).

Several controls are in place to ensure that access management is properly done:

- Users are identified through the use of a user ID/password combination using AWS and the 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 **(27).**
- The access to the production server is performed using SSM and is restricted to authorized personnel **(28).**
- The access to the deployment application required MFA and is restricted to authorized personnel **(29).**
- Access to production is performed only through VPN through authorized IP addresses. Access is performed using two factor authentication **(30).**
- Developers do not have access to the production and database environments. Specific developers can be granted access for specific projects. The access is restricted to authorized personnel. These accesses are logged and reviewed **(32).**
- 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 **(33).**
- Access to the source control tool is performed using MFA and is restricted to authorized personnel **(34).**
- Permissions to the different environments (production, databases and applications) are reviewed, approved and documented by the Cybord management on a quarterly basis **(36).**
- The permission to approve merge requests and to deploy is restricted to authorized personnel **(50).**
- Strict firewall rules are configured to protect network access and allow access to approved services. Access to the firewall management tool is restricted to authorized personnel **(40).**

Recertification of Access Permissions

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

Revocation Process

Terminated employees complete a termination clearance process on their last day at Cybord while the termination notification is documented and accessible within the Cybord Internal IT management ticket system. This process includes revocation of access permissions to the systems and premises and the return of the property, data and equipment. Also, terminated employees who had access to the production environment have their permissions removed and company equipment returned in a timely manner **(31).**

Production Environment Logical Access

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

Employees are provided with the minimal access rights required to carry out their duties. New employees are granted access to the different environments by a ticketing system process and subject to manager approval **(35).** A detailed ticket is opened in the IT management ticketing system using a new hire template. This template includes all user detailed permissions.

Remote Access

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

Physical Access and Visitors

Cybord recognizes the significance of physical security controls as a key component in its overall security program. Physical access to the offices is restricted to authorized personnel using a secured password according to the physical access policy **(37).** Physical access methods, procedures and controls have been implemented to help prevent unauthorized access to data, assets and restricted areas. Additionally, visitors to the Cybord office are accompanied while on premises **(38).**

Software Development Lifecycle (SDLC) Overview

The software development lifecycle consists of the following stages:

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

Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved within the change management application. Change management tickets are prioritized and labeled based on development phase and urgency **(47).** Product requirements are constantly being collected from customers and from market research by Cybord Product Managers. These requirements combined with additional engineering improvement requirements are discussed by R&D managers and Product Managers and are converted to a Product Requirements Document (PRD) that contains more specific description of required features and changes. Moreover, there is a documented change management policy. The policy is reviewed and approved on an annual basis **(46).** The R&D Managers review the PRD and provide a high-level effort estimation for every feature. The product managers work with the R&D managers to create a prioritized features list based on the effort estimation and required timeline of the release. The Release Manager collects the features list, validates the total effort vs teams foreseen progress and creates a release plan specifying integration dates, Feature Freeze and Code Freeze dates as well as the release date of 1st release candidate to PS.

R&D Engineers are engaged with ongoing enhancements of the product functionality. Each engineer implements Unit Testing to every new coded software module in accordance with Unit Tests guidelines document. Cybord performs unit testing using a dedicated tool. R&D engineer's check-in their respective code to a common source control system that provides extensive version tracking functionality and other software building abilities. All changes added to the Source Control contain information linking them to the relevant features and bugs. Code changes are reviewed along with the pull request performed by the 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 **(49).** Unit Tests are maintained according to product changes and enhanced based on bugs that were detected in previous product versions. Additionally, automation tests are performed using a dedicated tool on a regular basis in order to identify issues within the application **(51).** Check-in of code triggers Unit testing process and if passed successfully, a new build is created, and automated tests are executed on it. A successful test status is required to continue in the SDLC process **(52).** Moreover, tickets in the change management tool are connected to the source control tool in order to link the request to the code change **(48).**

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

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

Monitoring the Change Management Processes

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

Infrastructure Change Management Overview

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

The request is reviewed and approved by the Director of IT and Information Security. Emergency changes are performed and updated as part of hot fixes, which follow the same process as described above though the timeframe may be shortened, and approvals may be provided after the change was already performed.

Description of the Production Environment

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

AWS: Cybord's infrastructure runs on top of AWS's Infrastructure as a Service (IaaS) and utilizes various services such as: (1) EC2, (2) S3, (3) RDS (4), Kafka, (5) EKS, (6) CloudFront, which is the AWS's CDN, and more. These services are designed to make web-scale computing easier for Cybord.
AWS's web service interface (AWS Console) allows Cybord to obtain and configure capacity. It provides Cybord with control of computing resources and runs on AWS's computing environment. EC2 reduces the time required to obtain and boot new server instances to minutes, allowing to quickly scale capacity, both up and down, as computing requirements change. The use of EC2 allows to:

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

Production Environment

The processes described below are executed within Cybord's production environment, which is hosted in Amazon Web Services (AWS) Virtual Private Cloud located globally. The facilities comply with standards of quality, security, and reliability that enable Cybord to provide its' services in an efficient and stable manner.
Note: Controls performed by the data center service providers are not included in the scope of this report. The production environment is completely separated from the corporate environment and follows strict access and data processing procedures and processes. The environment is managed by a selected few Security personnel who use 2FA to connect using a dedicated AWS workspace.
All Cybord users who connect to the customers' VPCs for support purposes should login via a named workspace. All authentication is performed with a SAML provider. Customers' data is encrypted at test and in transfer. Access of Cybord personnel as well as customers is further restricted by IP filtering. Additionally, 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 **(25).**

Network Infrastructure

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

- Application layer security, including:
  - Various authentication schemas such as multi-factor authentication (MFA), unique ID and complex password policy.
  - Logical security.

  - Penetration testing.
  - IP address source restriction.
  - Customers data encryption at-rest and in transit.
- Network and infrastructure security, including:
  - Network architecture.
  - Risk management.
  - AWS data centers.
  - Cloud operation security (change management, monitoring and log analysis).

Web, Application and Service Supporting Infrastructure Environment

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

Production Monitoring

Cybord 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 Cybord personnel are notified of events related to the security, availability, or confidentiality of service to clients **(26).** Cybord's production network encompasses numerous components including web services, application and data server types, database, monitoring tools, and redundant network equipment provided as part of the AWS services. In addition, to improve service availability to clients and support the operations of the Cybord environments, Cybord maintains a dedicated Security department. The Security department is responsible for ongoing work on the production environment and investigating escalated issues. The production environment, including the servers and application, is monitored 24/7/365 by the NOC and Security team. Key Cybord staff members are notified of events related to the security, availability or confidentiality of service to clients.

Security and Architecture

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

Data Center Security

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

- **Redundancy** - The data centers are designed to anticipate and tolerate failure while maintaining service levels with core applications deployed to multiple regions.
- **Fire Detection and Suppression** – Automatic fire detection and suppression equipment has been installed to reduce risk.
- **Redundant Power** – the data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and Uninterruptable Power Supply (UPS) units provide back-up power in the event of an electrical failure. Data centers use generators to provide back-up power for the entire facility.
- **Climate and Temperature Controls** – maintain a constant operating temperature and humidity level for all hardware.

- **Physical access -** AWS recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures and controls have been implemented to help prevent unauthorized access to data, assets and restricted areas.

In addition, Cybord 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 Cybord to address the CUECs **(39).**

Infrastructure Security

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

Application Security

- **Penetration Testing** - An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved **(42).** The penetration tests include, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own. In addition, security scans are performed on a semi-annual basis. The penetration tests and security scans are performed by a reputable third-party vendor.
- **Vulnerabilities Management** - Web application architecture and implementation follow OWASP guidelines. The application is regularly tested for common vulnerabilities (such as CSRF, XSS, SQL Injection). Also, vulnerability scans are performed in order to detect potential security breaches. Vulnerabilities are tracked until resolution. Reports are created and sent to the security team **(41).**
- **Segregation of Customer Data** - Cybord employs a login system and authorization mechanism based on industry best practices. During each user request, a validation process is performed through encrypted identifiers to ensure that only authorized users gain access to the specific data. The process is validated by third-party security consultants yearly.

Operational Security

- ***Configuration and Patch Management* -** Cybord employs a centrally managed configuration management system, including infrastructure-as-code systems through which predefined configurations are enforced on its servers, as well as the desired patch levels of the various software components**.**
- ***Security Incident Response Management* -** Cybord has a security incident response management policy. Incidents trigger tickets and are tracked to resolution **(44).** Whenever a security incident of a physical or electronic nature is suspected or confirmed, Cybord's engineers are instructed to follow appropriate procedures. Customers and legal authorities will be notified as recurred by Privacy regulations.
- ***Antivirus*** - Antivirus software is installed on workstations, laptops, and servers supporting such software. Cybord uses a centralized management tool in order to receive alerts of the antivirus status **(43).** The employees' laptops are encrypted with the use of a 256-bit AES encryption.
- ***Unified Endpoint Management*** - XXX use a dedicate tool that implemented an Agent in advance on the company's endpoint in order to monitor and control the updates, data, content, configuration and encryption of the asset. The company Security Policy is enforced using a dedicate tool.

Human Resource Security

- ***Security Awareness Training*** - Employees go through annual security awareness training based on the Cybord security policy **(10).** The training ensures that each group of employees receive security training according to its technical knowledge and its needs.
- ***Secure Coding Standards and Training*** - Cybord's R&D team is regularly trained in secure coding practices such as CERT Oracle Secure Coding Standard for Java and the OWASP top 10. Furthermore, it is involved with analyzing penetration test results and defining the 'lessons learned'.

Data Encryption

- ***Data in transit*** - all traffic between the customer and the Cybord platform is encrypted through TLS with only the most secure algorithms enabled. Encryption between Cybord customers and the Application and between Cybord sites is enabled using an authenticated TLS tunnel. Connections to the Cybord network and databases are obtained through a secured IPSEC tunnel, only accessible from within the production network. Clients' sessions and interactions are encrypted using 256bit SSL V3/TLS HTTPS. Internet traffic is encrypted using high class level certificates based on the PKI infrastructure. Cybord uses encryption to supplement other measures used to protect data-at-rest when such protections are deemed appropriate based on assessed risk. Processes are in place to protect encryption keys during generation, storage, use, and destruction.
- ***Data at rest*** - Encrypted based on AWS's data at rest encryption policies which adhere to the following: Several layers of encryption to protect customer data at rest in Amazon Web Services products. Customer passwords are encrypted within the database **(53).** Also, interactions between customers and the Cybord platform are performed by using an encrypted channel based on an authenticated SSL connection **(54).** Data stored in AWS is encrypted at the storage level using AES256 Customer content stored at rest is encrypted, without any action required from the customer, using one or more encryption mechanisms. Data for storage is split into chunks, and each chunk is encrypted with a unique data encryption key. These data encryption keys are stored with the data, encrypted with ("wrapped" by) key encryption keys that are exclusively stored and used inside Amazon's central Key Management Service. Amazon's Key Management Service is redundant and globally distributed. A common cryptographic library is used to implement encryption consistently across almost all Google Cloud Platform products. Because this common library is widely accessible, only a small team of cryptographers needs to properly implement and maintain this tightly controlled and reviewed code.

Support

Cybord's customer support procedures are designed to handle and resolve issues and requests promptly. This includes issues that are internally identified, or issues submitted by clients. Cybord provides its clients with three types of support. Cybord customers choose either the Standard support level, Premium support level or Customized support level (as per customer request). All three types are available 24/7/365 via support mail, support hotline and customer support portal.

Ticketing and Management

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

Incident Management Process

A helpdesk application is available to Cybord employees to report breaches in system security, availability, and confidentiality. New employees are trained in this application at the start of their employment. The process is initiated when a new ticket is submitted in the helpdesk application or through emails. The company has a procedure and process in place to raise and manage Information Security Incidents. Incidents are classified according to the level of urgency and

importance. Incidents can be submitted into the system following a customer-identified issue, through both manual and automated proactive checks, or automatically through an email request. The application has pre-defined steps assigned to a pre-defined group of employees. The completion of each step is recorded in the application. When an incident is submitted, an email is sent to the IT and Information Security Director. Resources are allocated in order to investigate the incident and resolve the issue. The IT and Information Security Director is responsible for escalating critical incidents and perform Lesson Learnt reviews. By procedure and according to a strict SLA, Incident notifications are sent to customers in the case that their data has been impacted.

Escalation Process

Cybord's goal is to resolve issues in an efficient manner. The issue is tracked and updated in the support ticketing system. The escalation process is defined and documented by Customer Support. Tickets are escalated as deemed necessary to Security, R&D or Technical Services teams. Service interruptions and maintenance notifications are sent to customers and employees **(23).** Service interruptions are communicated to clients using e-mail based on the escalation procedures and Service Level Agreement (SLA) notification thresholds. In addition, response time to customer issues is defined in the SLA agreement. The agreement is communicated to the customers as part of the contract **(24).** Moreover, to maintain visibility on current support issues and potential problem trends, support metrics (including Key Performance Indicators) are generated from the support application and sent to Company's stakeholders on a regular basis.

Security Procedures

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

Database Backup

Cybord's databases are hosted at AWS. And fully weekly and monthly. The backup system automatically generates a backup log. In case of failure, a notification is sent to the Operation team. The company hold replica to each data center for high-availability standards in case of a disaster.

Restoration

Backup data captured as part of the daily, weekly and monthly backup procedures is restored automatically into a separate environment in order to determine the integrity of data and potential data recovery issues. A log of the restoring process is sent to the Director of Operations for review. Additionally, a restore process is performed and documented on an annual basis **(20).**

Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP)

Cybord has implemented a Disaster Recovery Plan and a Business Continuity Plan. The plans are reviewed annually **(21).** Additionally, Cybord has developed a Business Continuity Plan to enable the company to continue to provide critical services in case of a disaster. Cybord maintains a backup server's infrastructure at a separate location within the AWS environments. The backup server's infrastructure has been designed to provide clients with business-critical services until the disaster has been resolved and the primary system is fully restored. The alternative processing environment is wholly managed by appropriate Cybord personnel, as is the case with the primary production environment.

Monitoring Usage

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

Confidentiality Procedures

Customer confidentiality is key factor in Cybord. As such, Cybord has implemented security measures to ensure the confidentiality of its customer's sensitive personal information. The security measures aim to prevent unauthorized access, disclosure, alteration or destruction of sensitive personal information. In addition, connections to the Cybord network and databases are obtained through a secured IPSEC tunnel, only accessible from within the production network. In addition, business partners are required to sign an agreement containing a confidentiality clause **(55).** Also, upon customer request at the end of a contract agreement, Cybord will dispose of customer confidential information **(56).** Moreover, Cybord has implemented a vendor management policy which details the vendor termination process. The policy is reviewed and approved annually **(22).**

Subservice Organization Carved-out controls: Amazon Web Services ('AWS')

The subservice organization is expected to:

- Implement controls to enable security and monitoring tools within the production environment.
- Implement logical access security measures to infrastructure components including native security or security software and appropriate configuration settings.
- Restrict the access to the virtual and physical servers, software, firewalls and physical storage to authorized individuals and to review the list of users and permissions on a regular basis.
- Implement controls to:
    - Provision access only to authorized persons.
    - Remove access when no longer appropriate.
    - Secure the facilities to permit access only to authorized persons.
    - Monitor access to the facilities.
- Be consistent with defined system security as it relates to the design, acquisition, implementation, configuration modification, and management of infrastructure and software.
- Maintain system components, including configurations consistent with the defined system security, related policies.
- Provide that only authorized tested and documented changes are made to the system.
- Implement and maintain procedures exist and measures consistent with the risk assessment to protect the system against potential risks (for example, environmental risks, natural disasters, and routine operational errors and omissions) that might impair system processing integrity.

Cybord's User Entity Responsibilities

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

Criteria and controls

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 Cybord. The testing performed by Kost Forer Gabbay and Kasierer (KFGK) and the results of 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.

Description of Criteria and controls

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 Cybord Ltd.

Control Environment

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

#	Controls specified by the Company
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to Cybord's employees within the Cybord shared folders.
7	Job descriptions are documented and maintained within the Cybord website. Candidates go through screening and appropriate reference checks.
55	Business partners are required to sign an agreement containing a confidentiality clause.

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
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. Meeting minutes are retained.

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
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. Meeting minutes are retained.
2	The management of the company meets on a weekly basis to discuss on-going issues and updates. Meeting minutes are retained.
3	An organizational chart is documented and approved by management that clearly defines management authorities and reporting hierarchy.
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to Cybord's employees within the Cybord shared folders.

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
6	An information security policy is documented, reviewed and approved by Cybord management on an annual basis. The security policy is available to Cybord employees within the shared folders.
7	Job descriptions are documented and maintained within the Cybord website. Candidates go through screening and appropriate reference checks.
8	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different Cybord policies and work procedures.
10	Employees go through annual security awareness training based on the Cybord security policy.
11	Personnel responsible for the design, development, implementation, and operation of systems affecting security, availability, confidentiality, undergo training on an ad-hoc basis.

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
3	An organizational chart is documented and approved by management that clearly defines management authorities and reporting hierarchy.
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to Cybord's employees within the Cybord shared folders.
8	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different Cybord policies and work procedures.
11	Personnel responsible for the design, development, implementation, and operation of systems affecting security, availability, confidentiality, undergo training on an ad-hoc basis.
14	Employees go through a feedback process on at least an annual basis. The feedback reports are retained with the employee personal record.

Communication and Information

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

#	Controls specified by the Company
16	Risks and threats are evaluated by key Cybord stakeholders during an annual meeting. Action items are documented within minutes of the meeting.

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
4	A description of the Cybord system and its boundaries is documented and communicated to Cybord employees and to external users through the website.
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to Cybord's employees within the Cybord shared folders.
6	An information security policy is documented, reviewed and approved by Cybord management on an annual basis. The security policy is available to Cybord employees within the shared folders.
8	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different Cybord policies and work procedures.
10	Employees go through annual security awareness training based on the Cybord security policy.
13	New features are communicated to employees through the internal portal.
44	Cybord has a security incident response management policy. Incidents trigger tickets and are tracked to resolution.
45	Root cause analysis is performed following security incidents.

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

#	Controls specified by the Company
4	A description of the Cybord system and its boundaries is documented and communicated to Cybord employees and to external users through the website.
12	New features are communicated to customers, if relevant, through emails or dedicated meetings.
23	Service interruptions and maintenance notifications are sent to customers and employees.
44	Cybord has a security incident response management policy. Incidents trigger tickets and are tracked to resolution.
45	Root cause analysis is performed following security incidents.

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
16	Risks and threats are evaluated by key Cybord stakeholders during an annual meeting. Action items are documented within minutes of the meeting.
17	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.

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
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. Meeting minutes are retained.
2	The management of the company meets on a weekly basis to discuss on-going issues and updates. Meeting minutes are retained.

#	Controls specified by the Company
16	Risks and threats are evaluated by key Cybord stakeholders during an annual meeting. Action items are documented within minutes of the meeting.
17	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.

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
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. Meeting minutes are retained.
2	The management of the company meets on a weekly basis to discuss on-going issues and updates. Meeting minutes are retained.
16	Risks and threats are evaluated by key Cybord stakeholders during an annual meeting. Action items are documented within minutes of the meeting.
17	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.

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
20	A restore process is performed and documented on an annual basis.
22	Cybord has implemented a vendor management policy which details the vendor termination process. The policy is reviewed and approved annually.
41	Vulnerability scans are performed in order to detect potential security breaches. Vulnerabilities are tracked until resolution. Reports are created and sent to the security team.

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
6	An information security policy is documented, reviewed and approved by Cybord management on an annual basis. The security policy is available to Cybord employees within the shared folders.
23	Service interruptions and maintenance notifications are sent to customers and employees.
24	Response time to customer issues is defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.
25	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.
26	Cybord 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 Cybord personnel are notified of events related to the security, availability, or confidentiality of service to clients.

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
23	Service interruptions and maintenance notifications are sent to customers and employees.
24	Response time to customer issues is defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.
25	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.
26	Cybord 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 Cybord personnel are notified of events related to the security, availability, or confidentiality of service to clients.
44	Cybord has a security incident response management policy. Incidents trigger tickets and are tracked to resolution.

#	Controls specified by the Company
45	Root cause analysis is performed following security incidents.

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
16	Risks and threats are evaluated by key Cybord stakeholders during an annual meeting. Action items are documented within minutes of the meeting.

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
6	An information security policy is documented, reviewed and approved by Cybord management on an annual basis. The security policy is available to Cybord employees within the shared folders.
10	Employees go through annual security awareness training based on the Cybord security policy.

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
3	An organizational chart is documented and approved by management that clearly defines management authorities and reporting hierarchy.
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to Cybord's employees within the Cybord shared folders.
6	An information security policy is documented, reviewed and approved by Cybord management on an annual basis. The security policy is available to Cybord employees within the shared folders.
22	Cybord has implemented a vendor management policy which details the vendor termination process. The policy is reviewed and approved annually.
46	There is a documented change management policy. The policy is reviewed and approved on an annual basis.

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
27	Users are identified through the use of a user ID/password combination using AWS and the 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.
28	The access to the production server is performed using SSM and is restricted to authorized personnel.
29	The access to the deployment application required MFA and is restricted to authorized personnel.
30	Access to production is performed only through VPN through authorized IP addresses. Access is performed using two factor authentication.
33	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.
40	Strict firewall rules are configured to protect network access and allow access to approved services. Access to the firewall management tool is restricted to authorized personnel.
50	The permission to approve merge requests and to deploy is restricted to authorized personnel.
53	Customer passwords are encrypted within the database.

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
8	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different Cybord policies and work procedures.
30	Access to production is performed only through VPN through authorized IP addresses. Access is performed using two factor authentication.
31	Terminated employees who had access to the production environment have their permissions removed and company equipment returned in a timely manner.
32	Developers do not have access to the production and database environments. Specific developers can be granted access for specific projects. The access is restricted to authorized personnel. These accesses are logged and reviewed.
35	New employees are granted access to the different environments by a ticketing system process and subject to manager approval.
36	Permissions to the different environments (production, databases and applications) are reviewed, approved and documented by the Cybord management on a quarterly basis.

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
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to Cybord's employees within the Cybord shared folders.
31	Terminated employees who had access to the production environment have their permissions removed and company equipment returned in a timely manner.
35	New employees are granted access to the different environments by a ticketing system process and subject to manager approval.
36	Permissions to the different environments (production, databases and applications) are reviewed, approved and documented by the Cybord management on a quarterly basis.

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
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to Cybord's employees within the Cybord shared folders.
37	Physical access to the offices is restricted to authorized personnel using a secured password according to the physical access policy.
38	Visitors to the Cybord office are accompanied while on premises.

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
37	Physical access to the offices is restricted to authorized personnel using a secured password according to the physical access policy.
38	Visitors to the Cybord office are accompanied while on premises.

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

#	Controls specified by the Company
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. Meeting minutes are retained.
34	Access to the source control tool is performed using MFA and is restricted to authorized personnel.
43	Antivirus software is installed on workstations, laptops, and servers supporting such software. Cybord uses a centralized management tool in order to receive alerts of the antivirus status.
54	Interactions between customers and the Cybord platform are performed by using an encrypted channel based on an authenticated SSL connection.

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
28	The access to the production server is performed using SSM and is restricted to authorized personnel.
29	The access to the deployment application required MFA and is restricted to authorized personnel.
30	Access to production is performed only through VPN through authorized IP addresses. Access is performed using two factor authentication.
34	Access to the source control tool is performed using MFA and is restricted to authorized personnel.
43	Antivirus software is installed on workstations, laptops, and servers supporting such software. Cybord uses a centralized management tool in order to receive alerts of the antivirus status.

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
39	Cybord 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 Cybord to address the CUECs.
41	Vulnerability scans are performed in order to detect potential security breaches. Vulnerabilities are tracked until resolution. Reports are created and sent to the security team.
42	An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved.
43	Antivirus software is installed on workstations, laptops, and servers supporting such software. Cybord uses a centralized management tool in order to receive alerts of the antivirus status.

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
41	Vulnerability scans are performed in order to detect potential security breaches. Vulnerabilities are tracked until resolution. Reports are created and sent to the security team.
42	An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved.

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
25	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.
26	Cybord 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 Cybord personnel are notified of events related to the security, availability, or confidentiality of service to clients.
42	An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved.
43	Antivirus software is installed on workstations, laptops, and servers supporting such software. Cybord uses a centralized management tool in order to receive alerts of the antivirus status.

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
25	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.
26	Cybord 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 Cybord personnel are notified of events related to the security, availability, or confidentiality of service to clients.

#	Controls specified by the Company
41	Vulnerability scans are performed in order to detect potential security breaches. Vulnerabilities are tracked until resolution. Reports are created and sent to the security team.
44	Cybord has a security incident response management policy. Incidents trigger tickets and are tracked to resolution.
45	Root cause analysis is performed following security incidents.

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
41	Vulnerability scans are performed in order to detect potential security breaches. Vulnerabilities are tracked until resolution. Reports are created and sent to the security team.
44	Cybord has a security incident response management policy. Incidents trigger tickets and are tracked to resolution.
45	Root cause analysis is performed following security incidents.

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

#	Controls specified by the Company
22	Cybord has implemented a vendor management policy which details the vendor termination process. The policy is reviewed and approved annually.
23	Service interruptions and maintenance notifications are sent to customers and employees.
41	Vulnerability scans are performed in order to detect potential security breaches. Vulnerabilities are tracked until resolution. Reports are created and sent to the security team.
44	Cybord has a security incident response management policy. Incidents trigger tickets and are tracked to resolution.
45	Root cause analysis is performed following security incidents.

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
46	There is a documented change management policy. The policy is reviewed and approved on an annual basis.
47	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved within the change management application. Change management tickets are prioritized and labeled based on development phase and urgency.
48	Tickets in the change management tool are connected to the source control tool in order to link the request to the code change.
49	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.
50	The permission to approve merge requests and to deploy is restricted to authorized personnel.
51	Automation tests are performed using a dedicated tool on a regular basis in order to identify issues within the application.
52	A successful test status is required to continue in the SDLC process.

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
18	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.
44	Cybord has a security incident response management policy. Incidents trigger tickets and are tracked to resolution.
45	Root cause analysis is performed following security incidents.

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

#	Controls specified by the Company
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. Meeting minutes are retained.
2	The management of the company meets on a weekly basis to discuss on-going issues and updates. Meeting minutes are retained.
9	New employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses.
16	Risks and threats are evaluated by key Cybord stakeholders during an annual meeting. Action items are documented within minutes of the meeting.
19	Cybord assesses on an annual basis, the risks that vendors and business partners represent to the achievement of the company's objectives.
39	Cybord 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 Cybord to address the CUECs.
55	Business partners are required to sign an agreement containing a confidentiality clause.

Confidentiality

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

#	Controls specified by the Company
2	The management of the company meets on a weekly basis to discuss on-going issues and updates. Meeting minutes are retained.
9	New employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses.
29	The access to the deployment application required MFA and is restricted to authorized personnel.
54	Interactions between customers and the Cybord platform are performed by using an encrypted channel based on an authenticated SSL connection.

#	Controls specified by the Company
55	Business partners are required to sign an agreement containing a confidentiality clause.
27	Users are identified through the use of a user ID/password combination using AWS and the 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.
53	Customer passwords are encrypted within the database.
56	Upon customer request at the end of a contract agreement, Cybord will dispose of customer confidential information.

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

#	Controls specified by the Company
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to Cybord's employees within the Cybord shared folders.
56	Upon customer request at the end of a contract agreement, Cybord will dispose of customer confidential information.

****