Board Cloud Security Overview

board

Content

1. Introduction

This document provides an overview of Board's regulatory compliance, certifications and supporting processes that are designed to protect and secure data in Board Cloud. Board International (hereafter "The Company" or "Board") is committed to achieve, guarantee and maintain the principles of Confidentiality, Integrity and Availability and the trust of its customers. Board recognizes this is fundamental for customers' business activities. Board's priority is to form customer relationships built on trust by delivering transparency of Board's operations, policies and procedures that safeguard their data.

Board is committed to safeguarding and measuring its performance against and compliance with the highest security standards. Board continuously monitors current industry threats and uses them to improve its day-to-day information security policies and procedures as an integral part of its service. Board's robust security program carefully considers data protection matters across the service offered to the customers.

This document and the information thereon are confidential.
It is the property of Board and may only be used for the purpose for which it is supplied. No copying is authorized.

2. Board Cloud overview

Board Cloud provides all of Board's Intelligent Planning Platform capabilities plus all the benefits that a powerful cloud infrastructure can offer.

Backed by Microsoft Azure, Board Cloud reduces both setup time and maintenance overheads of your planning applications by offering world-class security, reliability, scalability, and performance.

Security is an integral part of how Board develops, tests and deploys the product and Cloud services. Exceptional levels of security are achieved using multiple methods and levels, covering aspects such as authentication, encryption, vulnerability monitoring and numerous other security technologies.

This document and the information thereon are confidential.
It is the property of Board and may only be used for the purpose for which it is supplied. No copying is authorized.

3. Board Cloud Deployment

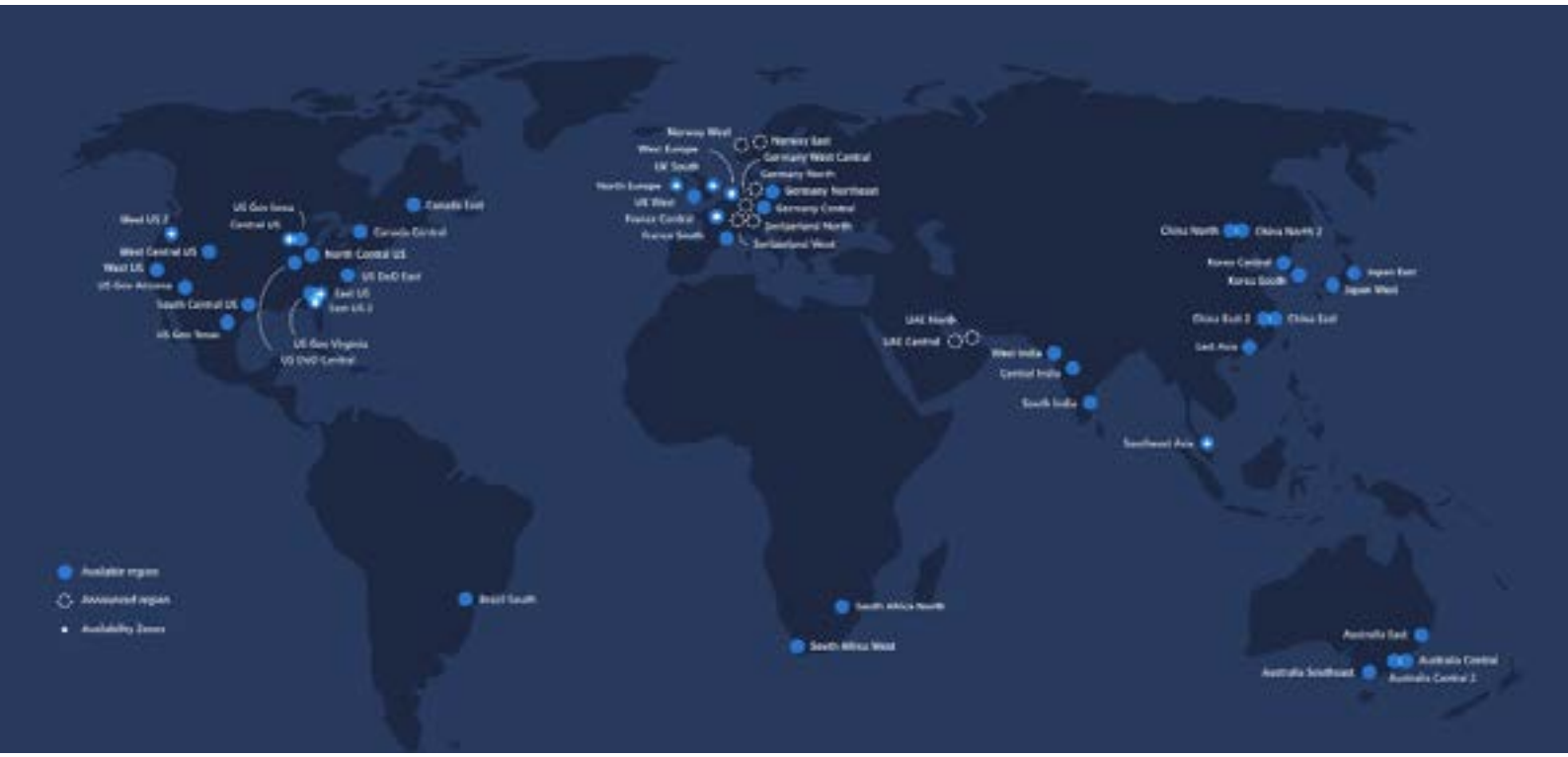
3.1 Data center and security

Board Cloud is deployed across Microsoft Azure data centers. Microsoft Azure's geographical coverage enables compliance with various local policies and regulatory requirements regarding the processing and storage of personal or financial data, ensuring the highest levels of security, reliability, transparency and compliance.
Microsoft Azure data centers comply with key industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, for security, availability, and reliability. They also meet a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2, along with country- or region-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS.

You can learn more about Microsoft's compliance offerings here.

This solid partnership enables Board to deploy Cloud solutions on servers strategically located to dramatically reduce potential latency issues encountered with some globally scaled cloud-based services.
Customers can select the most appropriate geographical location for their tenant environment from Board's list of supported Azure regions and data centers. Data storage may be limited to a single country, region or geographical area. (refer to Fig. 1 – Microsoft Azure Regions)

Fig. 1 – Microsoft Azure Regions



This document and the information thereon are confidential.
It is the property of Board and may only be used for the purpose for which it is supplied. No copying is authorized.

Officially supported Azure regions and data centers

Country	Region Name	State
Australia	Australia Central	Australia
Australia	Australia East	New South Wales
Australia	Australia Southeast	Victoria
Brazil	Brazil South	Brazil
Canada	Canada Central	Canada
India	Central India	India
US	Central US	Iowa
Hong Kong	East Asia	Hong Kong
US	East US	Virginia
US	East US 2	Virginia
France	France Central	France
Germany	Germany West Central	Germany
Japan	Japan East	Japan
US	North Central US	Illinois
Ireland	North Europe	Ireland
Norway	Norway East	Norway
South Africa	South Africa North	South Africa
US	South Central US	Texas
Singapore	Southeast Asia	Singapore
Switzerland	Switzerland North	Switzerland
United Arab Emirates	UAE North	United Arab Emirates
UK	UK South	UK
Netherlands	West Europe	Netherlands
India	West India	India
US	West US	California
US	West US 2	Washington

This document and the information thereon are confidential.
It is the property of Board and may only be used for the purpose for which it is supplied. No copying is authorized.

The list of supported Azure regions and data centers is constantly growing and, if necessary, customers can select Azure regions not on the list with the help and validation of Board's cloud team.
Microsoft adheres to rigorous security controls which govern its operations and support. Microsoft deploys combinations of preventive, defensive, and reactive controls including the following mechanisms to help protect against unauthorized developer and/or administrative activity:

- Tight access controls on sensitive data, including a requirement for two-factor smartcard-based authentication to perform sensitive operations.
- Combinations of controls that enhance independent detection of malicious activity.
- Multiple levels of monitoring, logging, and reporting.

Additionally, Microsoft conducts background verification checks of certain operations personnel and limits access to applications, systems, and network infrastructure in proportion to the level of background verification.
Microsoft Azure meets a broad set of international as well as regional and industry-specific compliance standards. Azure's adherence to the strict security controls contained in these standards is verified by rigorous third-party audits that demonstrate Azure services work with and meet world-class industry standards, certifications, attestations, and authorizations.

You can learn more about Microsoft Azure compliance offerings here.

Board takes advantage of its wide array of security tools and capabilities to address business objectives and industry standards and regulations.

This document and the information thereon are confidential.
It is the property of Board and may only be used for the purpose for which it is supplied. No copying is authorized.

4. Data Security

4.1 Customer Data

The Customer is the exclusive owner of the Customer Data loaded on the System.
The Customer has all rights, titles, and interests in and to all of the Customer Data.
Cloud Operations team members do not have access to customer data, except in the following two scenarios:

- **With the prior written consent of the Customer, to respond to System or technical problems,**
- **At the Customer's written request in accordance with the Customer's written instructions.**

4.2 Data Isolation

Board Cloud provides customers with one or more dedicated Board Platforms. Each Board Platform isolates tenant operation at the OS, database, and application server layer.

All software components are dedicated for each customer Platform and never shared across multiple customers.

4.3 Data Encryption

Board Cloud secures data both in transit and at rest using strong encryption algorithms. Board Cloud uses disk encryption to secure data at rest. All backups of customer information are also encrypted.
All the communication and data in Board are encrypted. Board uses digital SSL\TLS protocols for all connections and encryption at rest for all data storage.

- Data at rest is encrypted through AES 256-bit encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant.
- Data in transit is protected with TLS 1.2 using a 2048-bit RSA certificate with SHA256

The Customer can also decide to encrypt logs and data in each Data model using personal keys (Bring Your Own Key Encryption – BYOK).

This document and the information thereon are confidential.
It is the property of Board and may only be used for the purpose for which it is supplied. No copying is authorized.

5. Security controls on Board cloud

5.1 Board's service provisioning

Once the agreement is signed, the service provisioning of Board Cloud is performed.
Once the Cloud Operations team have successfully deployed the Board Cloud customer instance a series of emails are sent to the authorized customer contact appointed in the contract.
The process is as follows:

1. 1. An initial welcome email is sent. This email informs the primary customer contact that a subsequent email will follow with details of how to activate a new account on the Board Subscription Hub.
2. 2. A second email is then sent to the primary contact of the account with the activation link referenced in step 1. Once clicked, the user is taken to a screen in the Board Subscription Hub, from which they can create an account.
3. Once the account has been created (step 2), a third email is sent inviting the user to activate the new account. This is achieved by clicking on the activation link included in the email.

Once the customer completes the activation tasks outlined above, the provisioning is considered completed.

5.2 Single sign-on authentication

SSO ("Single Sign – On") allows application administrators to permit access to the Board Cloud Platform by integrating with customers' authentication mechanisms.

Board supports user authentication via external Identity Providers (IDPs) configured in the Board Subscription Hub.

Board fully supports Security Assertion Markup Language (SAML 2.0) and OpenID Connect (OIDC).

5.3 Customizable Password Policy

In the Subscription Hub, administrators can customize the login options of associated Platforms and create their own password and locking policy.

Default password complexity requirements for Board user accounts is as follows:

- **At least 8 characters**
- **At least one uppercase**
- **One digit character and one non-letter**
- **Expiration after 365 days**
- **History of last 5 passwords used**
- **Five login attempts: If a user types a wrong password five times, it is disabled for 30 minutes.**

This document and the information thereon are confidential.
It is the property of Board and may only be used for the purpose for which it is supplied. No copying is authorized.

5.4 Log & auditability

All access is monitored and logged.
Unauthorized processing of information is monitored using specific software that monitors cloud environments to maintain their availability and performance.

Additionally, advanced intrusion detection systems are also configured across all Cloud environments.
Access by all system administrators is logged. The log files are securely stored on an Azure repository.

Any access to the Cloud environment by the Board Cloud Operations team is also logged.
All customer end-user access is also logged and made available to Customer through the Board Cloud Administration Portal and the Subscription Hub, via dedicated Audit Log files.

The Customer also has the ability to encrypt their logs.

5.5 Board employee access and control

- **Only the Cloud Operations Team can access Board Cloud Resources. This access is permitted only with Two Factor Authentication (2FA) and access to any datacenter server and resources is further protected by an SSL VPN that uses a personal encryption certificate.**
- **Board employees do not have access to customer data: each member follows specific procedures and processes to ensure the highest levels of security.**

This document and the information thereon are confidential.
It is the property of Board and may only be used for the purpose for which it is supplied. No copying is authorized.

6. Business continuity management

Board has a well-defined Governance System for Information Security. This system has been defined in accordance with the rules and criteria provided by industry best practices and international reference standards (ISO).
An Information Security Management System created by Board also includes aspects of business continuity (as required by ISO - A17. Information security aspects of business continuity management) to ensure the availability and integrity of the service and any data stored within. To remain compliant with such requirements, the company has implemented and follows the controls, best practices and procedures detailed below:

- **Data event: Procedure to guarantee continuity and preventing data loss through the backup/restore strategies.**
- **System event: Controls and procedures to guarantee service continuity and restoration in case of failure.**
- **Monitoring policies and procedures are in place for addressing events relating to outages of critical services or data requiring immediate action. The monitoring system supervises the system health by analyzing both data and system events such as network capacity, hardware performance/ failure and cyber-attacks.**

Policies and controls have also been implemented specifically to manage redundancy and availability of data within the cloud environment, as explained hereafter:

Data Center redundancy and availability
Board Cloud is deployed exclusively on Microsoft Azure Data Centers around the world.
All Data Centers comply with key industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, for security, availability, and reliability. They also meet a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2, along with country- or region-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS.

The use of Azure Data Centers allows Board to:

- Isolate data within a desired region to comply with local policies and regulatory requirements with regards to processing and storage of personal or financial data.

- Choose a Data Center in proximity to the customer's user base.

Board Service redundancy and availability
Each customer has a dedicated environment which includes a pool of computing resources and storage areas. Redundancy and availability of resources pool is guaranteed through a multi-layer redundant architecture.

Board Data redundancy and availability
Customer data stored in the Shared storage area is replicated (three copies) within the same data center (where the live data is located) and additional backup copies of platform data are stored in a secondary datacenter within the associated Azure affinity region.

This document and the information thereon are confidential.
It is the property of Board and may only be used for the purpose for which it is supplied. No copying is authorized.

All data associated with Disaster Recovery (customer data, configuration data, environment settings, necessary to restore the full service) is organized over 3 layers:

1. Data center Layer

All infrastructure data, as environment configurations, settings, and resources images, are stored on a dedicated storage which is locally redundant and Geo-redundant.

2. Instance Layer

For each Platform, a full backup is performed once a day with the following retention policy:

- last 15 days rolling: snapshot of the entire virtual machine;
- last 3 months rolling: snapshot of the entire virtual machine taken on first day of the month.

All backup data are also replicated in a secondary datacenter within the associated Azure affinity region.

Customers can select different retention policies based on their needs: it is possible to have intraday recovery points and a Recovery Point Objective (RPO) less than 24 hours.

Customers can also perform full backups of their data using Board's self-service backup feature and schedule their own backup plan.

This document and the information thereon are confidential.
It is the property of Board and may only be used for the purpose for which it is supplied. No copying is authorized.

7. Information security incident management

The company follows a specific procedure to trace, manage and monitor any security related incident or events.
The primary aim is to ensure that the best possible levels of information security and highest level of service quality and availability are maintained.

This is achieved through the following:

- **The definition of adequate management structure to prepare, mitigate and respond to adverse events.**
- **The appointment of suitable personnel to respond to incidents with the necessary responsibility, authority, and competence to handle an accident and maintain the security of information.**
- **The development and approval of documented plans, response and recovery procedures detailing how the organization must handle an adverse event and how the security of information is maintained at a predetermined level, based on approved goals of managing information continuity.**

Information Security events must be promptly reported to the Information Security Officer.

In the event of a security data breach, the customer is notified. In a timely manner, a shared remediation plan is implemented to resolve the issue.

This document and the information thereon are confidential.
It is the property of Board and may only be used for the purpose for which it is supplied. No copying is authorized.

8. Board software development life cycle

Board incorporates security during the software development lifecycle.
Board has and follows an Agile system development methodology, composed of specific phases:

1. Analysis & Design

The development of the Board product and its characteristics starts with the collection and analysis of requirements. The R&D team considers each feature and determines the possible threats for this feature. Countermeasures are put in place to prevent and mitigate each threat.

2. Development

To perform all releases in a secure and safe way, the R&D team follows a dedicated IT Security measures checklist. The system is protected against the top 10 OWASP 'Open Web Application Security Project' threats.

3. Test (SecOps approach)

Test cases are created from a security perspective and executed during the development process. Testing includes system level, feature level, and penetration level. Test cases consider the end-to-end new product release to identify any security issues within the new product. Specific tests are conducted on code that contains the new features within the product.

4. Deploy

The R&D department is involved in the deployment phase through its vulnerability management process. Working with external security companies and customers to identify vulnerabilities within the deployed code, the team will assess any reported vulnerability and determine appropriate action. The goal is to identify areas of improvements, making the model an evolving entity that is updated on a regular basis.

All developers and testers follow a security training program to improve and implement the methodologies that allow to effectively apply security techniques aimed at minimizing the number and severity of threats. The Board R&D team follows detailed standards and techniques to make the security system work effectively.
Board enforces a process of Vulnerability Assessment/Penetration Testing to detect vulnerabilities, which is performed by an independent third party highly specialized in cybersecurity. This test is conducted at least once a year and on the occasion of each major release.

8.1 Security vulnerability response

Upon identification of any security vulnerability, Board can exercise commercially reasonable efforts to address the vulnerability in accordance with the following policy:

RATING*	CVSS SCORE	TIME GUIDELINE	VERSIONS
Low	0.1 – 3.9	Best effort	Latest shipping version
Medium	4.0 – 6.9	180 days	Latest shipping version
High	7.0 – 8.9	90 days	Latest shipping version & All supported versions
Critical	9.0 – 10.0	30 days	Latest shipping version & All supported versions

** Rating is established based on the current version of the Common Vulnerability Scoring System (CVSS) 3.1, an open industry standard for assessing the severity of computer system security vulnerabilities. For additional information on this scoring system, refer to https://en.wikipedia.org/wiki/CVSS*

In case of a zero-days vulnerability, Board puts in place all the necessary security mitigations and resolutions as soon as possible in order to avoid malicious exploitation of the internal software or external vendor's software, taking into account the recommendations of the specialized authorities and experts applying the main sector best practices.

9. Board Employees

Board addresses security at the initial recruitment stage. Security associated responsibilities are defined in employees' contracts and adherence is monitored throughout an individual's employment. All employees assigned to the R&D department are obliged to sign a confidentiality (non-disclosure) agreement.

Careful attention is paid to validate the references and the appropriate level of background checks. For Board, it is crucial to increase the level of expertise and to raise awareness for ensuring that law, guidelines and procedures relating to information security are complied with in full.

Board has in place various initiatives related to security topics to ensure that all employees are qualified for and have a precise understanding of their tasks and responsibilities. All employees undergo a regime of security training throughout the year. Content and features cover at least general security awareness, e-mail security, phishing awareness, GDPR Training, and secure coding.

At Board the information security awareness program is established in line with the organization's information security policies and covers general aspects such as:

- **The needs to become familiar with and comply with applicable information security rules as defined in policies, regulations, contracts, and agreements.**
- **Personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organization and external parties.**
- **Basic information security procedures and baseline controls (such as password security, malware controls, clear desks, and clear screen).**

10. Regulatory compliance & certifications

Board Cloud is designed and certified to meet compliance requirements.
As part of Board's commitment to maintaining a world-class security service, Board validates the effectiveness of its cloud security controls by auditing its environment using internationally recognized auditing standards.
Board has achieved the following certifications.

10.1 SOC 1 Type II

Board has successfully completed its SOC 1 Type II audit.
The SOC (Service Organization Controls) report conforms to SSAE 18 (Statement on Standards for Attestation Engagements No.18) and ISAE 3402 (International Standard on Assurance Engagement No.3402) auditing standards and provides guidance for auditors assessing Internal controls at a service organization, such as Board, that are likely to be relevant to customer's Internal control over financial reporting.

The report SOC 1 Type II is based on the suitability of the design and operating effectiveness of the IT controls on Board Cloud to achieve the related control objectives included in the description throughout a specified period.
The SOC1 audit is conducted annually by an independent third-party auditor. The report is available on request.

This document and the information thereon are confidential.
It is the property of Board and may only be used for the purpose for which it is supplied. No copying is authorized.

10.2 SOC 2 Type II

SOC 2 reports on controls at a service organization unrelated to financial reporting.
The focus is on standards important to the security, availability, or processing integrity of the service organization's system, and the confidentiality and privacy. A given SOC 2 report may be based on one or more trust principles.
The Board SOC 2 report focuses on the security and availability controls.

The SOC 2 Type II report includes a detailed description of tests of controls performed by the service auditor and the test results.
The controls are found in the Trust Services Principles and Criteria (TSP) Section 100 which is maintained by the American Institute of Certified Public Accountants (AICPA). The report is available on request.

10.3 SOC 3

The SOC 3 report is a public report. It is a short version of the SOC 2 Type II attestation report.
SOC 3 provides users and interested parties a report about the controls at the service organization related to security, availability, processing integrity, confidentiality, or privacy.
The SOC 3 report is created by the third-party company that performs the SOC 2 audit.
The SOC 3 report can be downloaded from the URL: https://www.board.com/en/governance-and-compliance

10.4 ISO/IEC 27001:2013

Board maintains an ISO/IEC 27001:2013 certification for **Board Cloud** to demonstrate its conformity with the defined requirements in the ISO/IEC 27001:2013 standard.
Jointly published by the International Standard Organization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27001:2013 is a globally recognized information security standard that provides organizations with requirements for an Information Security Management System (ISMS). The standard security model is based on three pillars: confidentiality, integrity, and availability of information assets. Each of those covers a different aspect of providing information security and protection.

An annual audit is conducted to validate compliance with the standard and a full certification occurs every three years.
Board's ISO/IEC 27001:2013 certificate is available for customer and prospect review.
The scope of certification is **"the design and development of Board platform for Business Intelligence, Performance Management and Analytics and its own installation, maintenance, and support through Cloud SaaS Service (Software as a Service)".**

Overall, Board has demonstrated its commitment to securely manage all processes related to Board Cloud, e.g. Lifecycle development process, provisioning of the Board Cloud service, legal and regulatory compliance and an ongoing monitoring of security of information. Moreover, Board has developed an organization–wide Information Management System (ISMS) based on the ISO 27001 Framework. It contains policies, procedures, guidelines, work instructions and checklists for internal use and distributed to all employees. The Information Security Officer (ISO) regularly reviews and updates the security policies. This review assesses the availability, confidentiality, and integrity of information assets, as well as conformance to the information security policy.

10.5 Cloud Security Alliance

The **Cloud Security Alliance (CSA)** is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.
Board International, as a CSA member, has completed the Cloud Security Alliance (CSA) STAR Level 1: CSA Star Self-Assessment - Consensus Assessments Initiative Questionnaire (CAIQ) released by the CSA. For more information, please refer to the following: STAR Registry Entries for Board International SA | CSA (cloudsecurityalliance.org)

This document and the information thereon are confidential.
It is the property of Board and may only be used for the purpose for which it is supplied. No copying is authorized.

11. Governance and risk management

Board conducts an annual risk assessment of security risks. As part of this process, security threats are identified and the risk from these threats is assessed.

The Risk Assessment phase begins with identifying risks, establishing a risk level by determining the likelihood of occurrence and impact, and finally, identifying controls and safeguards that reduce the impact of the risk to an acceptable level. According measures, recommendations and controls are put in place to mitigate the risks to the extent possible.
As part of the overall ISMS – Information Security Management System- Framework baseline security requirements are constantly being reviewed, improved, and implemented.

This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, as well as planning and tracking necessary corrective actions. Each version of the Information Security Policy and all subsequent updates are distributed to all relevant stakeholders. The information security Policy is made available to all new and existing staff for review. In the event that a significant change is required in the security requirements, the policy may be reviewed and updated outside the regular schedule.

This document and the information thereon are confidential.
It is the property of Board and may only be used for the purpose for which it is supplied. No copying is authorized.

12. About Board

Board's Intelligent Planning Platform delivers solutions that help over 2,000 organizations worldwide plan smarter - enabling actionable insights and better outcomes. Board helps leading enterprises discover crucial insights which drive business decisions and unify strategy, finance and operations through more integrated and intelligent planning to achieve full control of performance. Partnering with Board, global enterprises such as H&M, BASF, Burberry, Toyota, Coca-Cola, KPMG, and HSBC have digitally transformed their planning processes.

Founded in 1994, and now with 25 offices worldwide, Board International is recognized by leading analysts including BARC, Gartner, and IDC.

www.board.com

This document and the information thereon are confidential.
It is the property of Board and may only be used for the purpose for which it is supplied. No copying is authorized.

EN2209J

www.board.com