# Board Cloud Technical Reference

board

This document provides an overview of how Board manages and guarantees the continuity of its Cloud service and Board's regulatory compliance, certifications, and supporting processes that are designed to protect and secure data in the Board Cloud.

Board International (hereafter "The Company" or "Board") is committed to achieving, guaranteeing and maintaining the principles of confidentiality, integrity, and availability, in addition to the trust of its customers. Board recognizes that this is fundamental for customers' business activities.

Board's priorities are:

- 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.
- to ensure the continuity of the Board Cloud service to its customers in the event of disasters, failures, or malfunctions that may have a negative impact on the ability of Board to offer services according to acceptable levels of quality and readiness.

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 our customers.

# Table of Contents

# 1. About Board

The Board Enterprise Planning Platform powers financial and operational planning for more than 2,000 organizations worldwide. Industry leaders trust Board to turn complex data into better decisions with AI, analytics, and tailor-made solutions for enterprise-grade challenges.

Global brands including H&M, BASF, Burberry, Toyota, Coca-Cola, KPMG, and HSBC use Board to enhance workflows and strengthen their competitive edge.

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

www.board.com

# 2. Board Cloud

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

These geographically dispersed datacenters are managed and operated by Microsoft and, to ensure security, availability, and reliability, comply with key industry standards, such as: ISO/IEC 27001:2022, NIST SP 800-53, ISO 27017, HIPAA, FedRAMP, SOC 1 Type II, SOC 2 Type II, along with country- or region-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS.

## 2.1 Board Cloud Services

Board Cloud provides all of Board's Intelligent Planning Platform capabilities plus all the benefits that a powerful cloud infrastructure can offer. Board Cloud gives organizations the ability to adjust the technology to suit their business, rather than the other way around.

In the cloud era, Board is recognized as a cloud service provider as its core business, and the exposed services are consumed in a public cloud mode by the customer. The entire cloud infrastructure allows Board to deliver its service at any time and when it is needed by the customer. This is also possible because Board has identified which services are vital to maintaining the cloud service, even in the event of unexpected or unwanted events.

Thanks to its organizational, operational, and technical structure, Board ensures high availability through advanced monitoring and incident response, service support, and backup failover capabilities.

## 2.2 Board Cloud Solution

Such broad geographical coverage allows Board to comply with a large number of policies and regulatory requirements regarding the processing and storage of personal or financial data. Board Cloud helps companies deploy global rollouts by assisting organizations in the following areas:

**Simplifying business models**

**Standardizing global processes**

**Deploying across an industry standardized platform and interfacing technologies**

With **zero infrastructure investment** required, organizations only pay for what they use, making planning more cost-effective and less risky than ever before.

Board Cloud is available in **different languages**, such as English, French, German, Spanish, Italian, and Japanese.

Your organization-specific terminology can be translated in any language using Board's built-in Localization feature that allows users from different countries to see the same application dimensions and measures in a preferred language.

# 2.3 Cloud Architecture

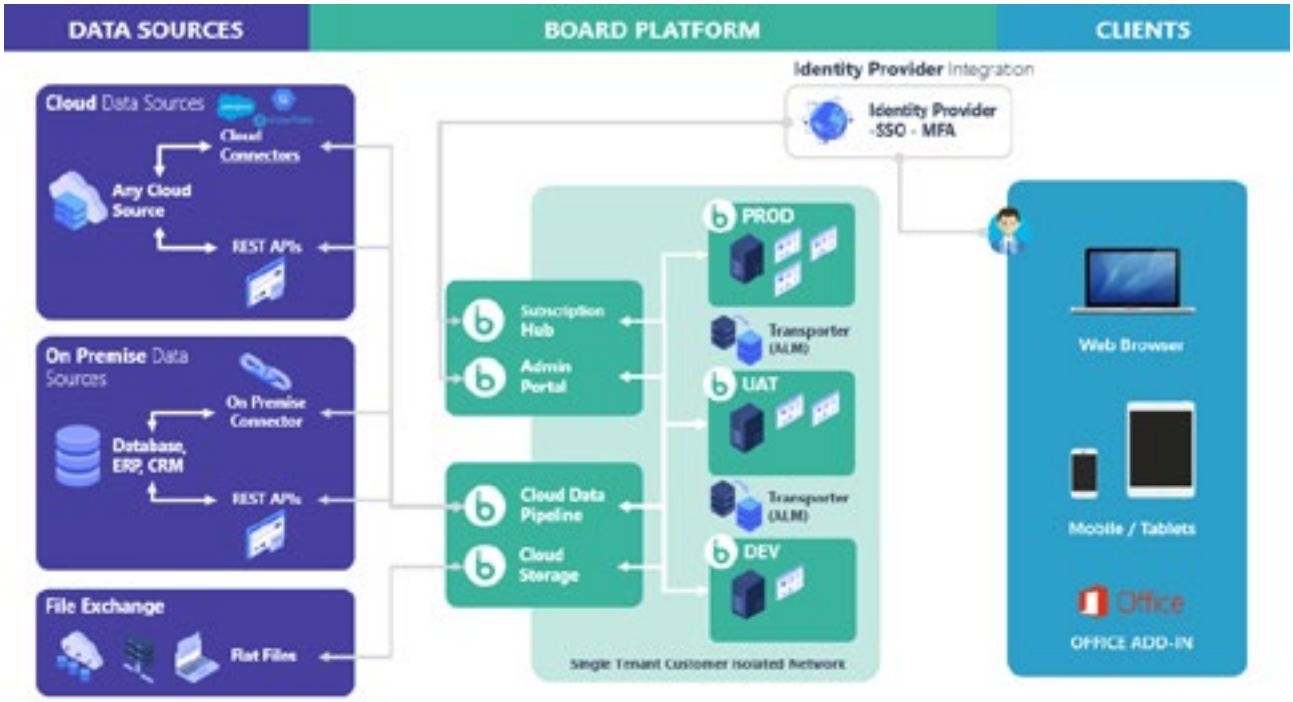
Board Cloud reduces both setup time and maintenance overheads of your planning applications by offering world-class security, reliability, scalability, and performance.

Board Cloud's globally spanning infrastructure supports enterprise level rollouts by providing robust levels of integration with many third-party systems such as ERPs, CRMs, Cloud applications, Data Warehouses, and many more.

Board Cloud provides one (or more) production instance(s) with the possibility to activate one or more Sandbox environments to be used for Development, User Acceptance Testing, and Pre-production instances, depending on the Customer's project requirements and policies. Board Cloud customers also have access to dedicated Subscription Hub and Cloud Administration portals, where they can manage their Board Cloud environment and carry out a range of administrative and management tasks.

The diagram below shows a high-level description of the Board Cloud Architecture.

***Fig. 1 – Board Cloud Architecture***




## 2.3.1 Dedicated Tenant

Each customer is provided with a dedicated tenant that houses their Board instances and data. Secure network segregation guarantees complete isolation from other tenants.

This architectural approach provides the following benefits:

- **Enhanced security:** A complete separation ensures the isolation of all customer data.
- **Superior reliability:** The performance of a customer's instance will never be impacted by any concurrent activity of another Board Cloud customer.
- **Version isolation:** Customers can upgrade their Cloud instances whenever it's needed, regardless of other customers' upgrade activity.

## 2.3.2 Subscription Hub

The Board Cloud Subscription Hub is an administration portal that allows you to carry out several user management tasks on multiple Board Cloud instances at once, such as handling user authentication and authorization.

The Subscription Hub makes it easier to manage all users and ensures a higher degree of efficiency while reducing administration efforts.

When using Board local authentication, you can import users in bulk and customize the password policy to meet your requirements or leverage a federated identity provider already in place within your organization and automatically sync user accounts and permissions through Board SCIM APIs.

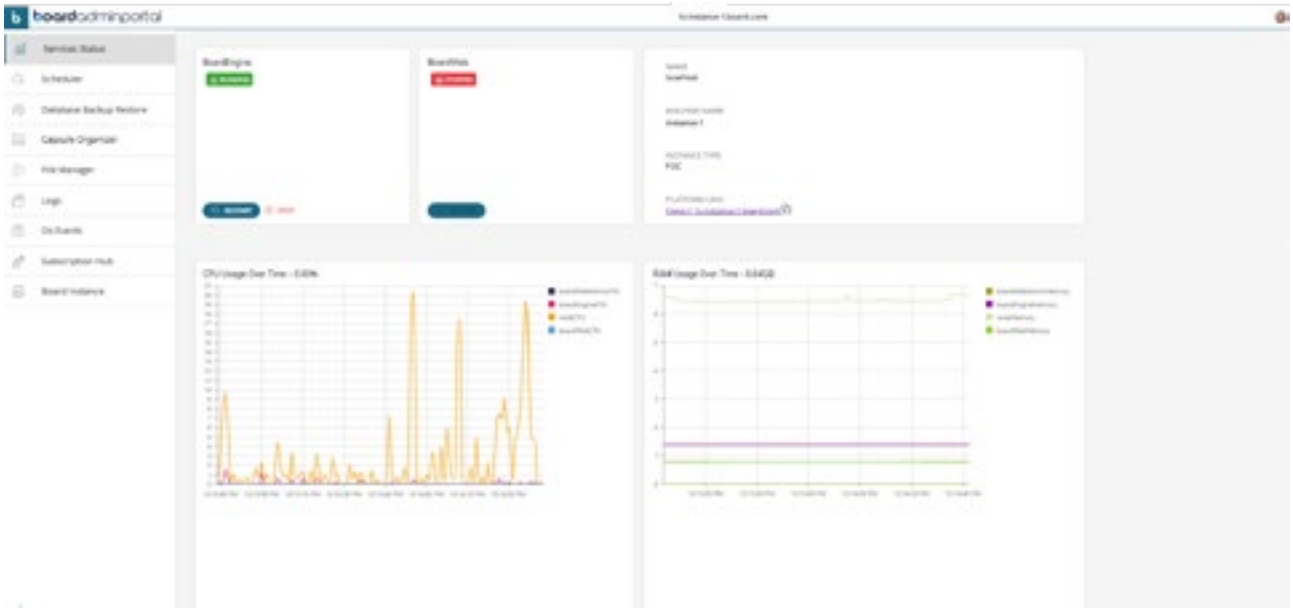
Board supports identity providers based on SAML2 and OIDC standards.

The Subscription Hub also allows you to set up and manage Board's Collaboration services, allowing users to connect, share, and work together on Cloud instances in the same, unified interface.

## 2.3.3 Cloud Administration Portal

The Cloud Administration Portal provides a full overview of each Board instance and allows customers to manage it.

***Fig. 2 – Cloud Administration Portal Dashboard***



The Cloud Administration portal offers many features and options, including:

- Platform\sandbox resource consumption monitoring
- Scheduling and management of administrative tasks, such as data import via Board Procedures
- Complete management of your data backups (preserve, archive and purge)
- Management of Capsule files and Folders in the instance
- Managing connections to your data sources and to the Cloud connector
- Access to the extensive range of Board logs and the instance level services event log

## 2.3.4 Instances Type

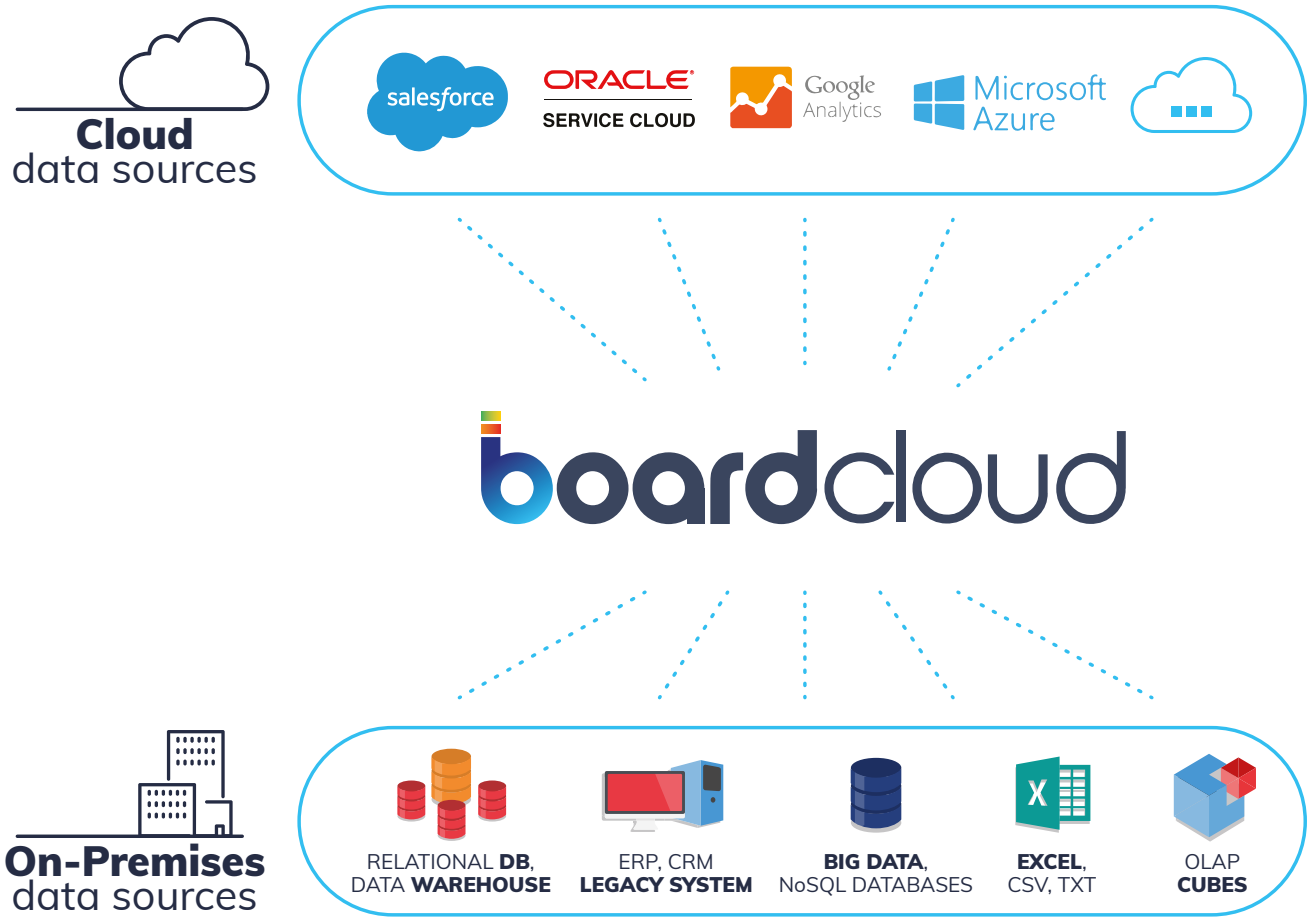
Each tenant contains one (or more) production instance(s) with the possibility to activate one or more Sandboxes to be used for Development, User Acceptance Testing, and Pre-production.

Platform and sandbox environments are technically similar, the distinction lies in their Service Level Agreement (SLA) for availability. In this context, platform environments are suitable for Board Cloud production solutions, and production data.

## 2.3.5 Data Integration and Cloud Connector

Board Cloud is designed to offer a seamless connection to on-premises and cloud data systems, allowing you to deliver planning solutions that fully leverage your existing software investments.

***Fig. 3 – Board Data Sources***




Board Cloud integration capabilities enable native external integrations with all major cloud storage systems, such as Amazon S3, Azure File\Blob storage, and Google storage. The Board Cloud connector enables the most complex integration scenarios, as it is specifically designed to allow Board applications to access external data sources, both on-premises or in the cloud.

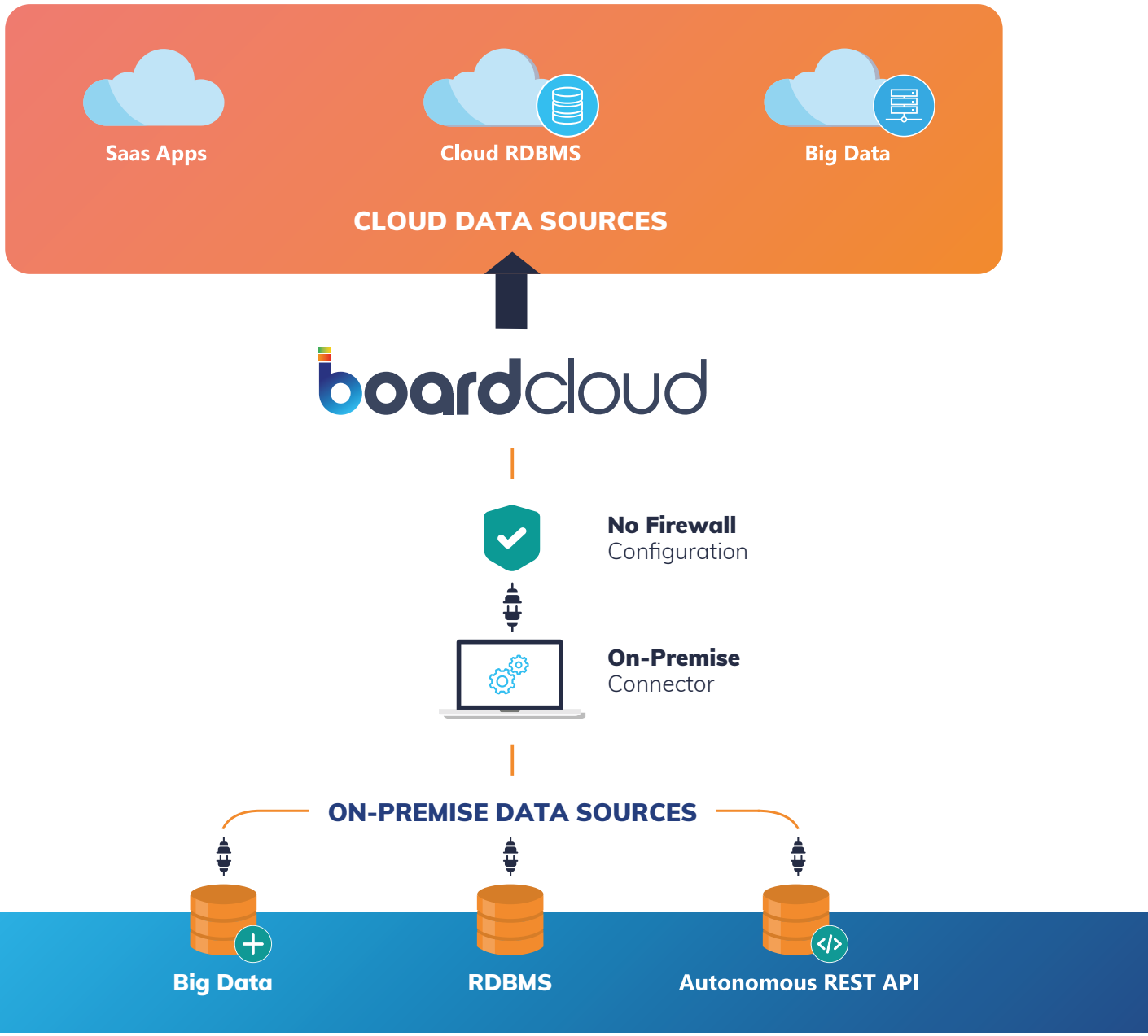
The Board Cloud Connector consists of two components:

- Hybrid Data Pipeline Cloud Service
- On-Premises Connector (for those data sources on the customer premise)

## Hybrid Data Pipeline Cloud Service

The Hybrid Data Pipeline is the main component of the Cloud connector, creating a web portal where the user can configure all the necessary connections and rules.

***Fig. 4 – Board Data Pipeline***



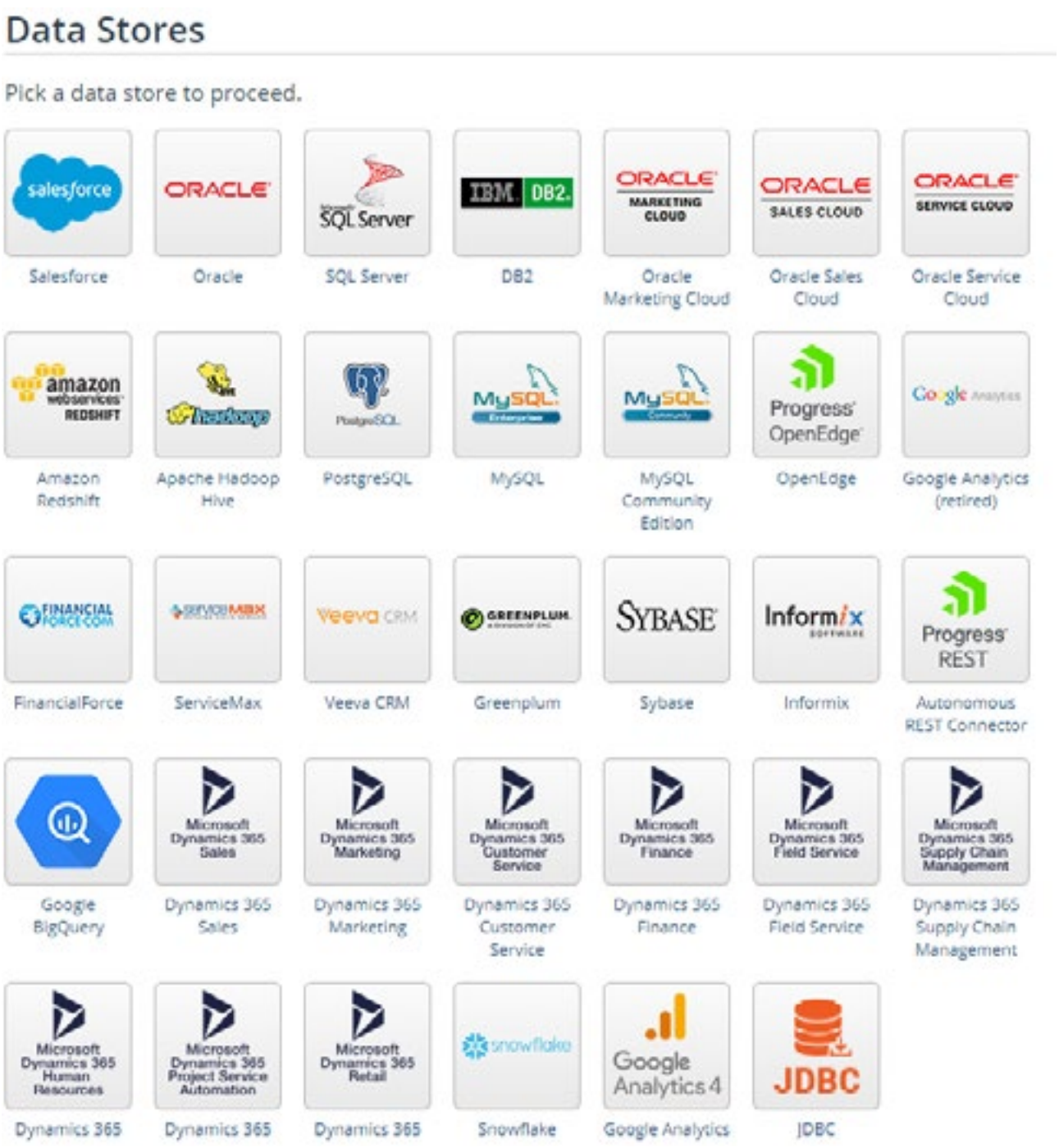

## On-Premises Connector

This component is installed remotely to allow Board applications to access source systems that reside behind customer firewalls. It provides the services needed to securely move data from on-premises applications to Board Cloud. This component connects to the Hybrid Data Pipeline Service using a secure HTTPS connection without requiring additional firewall configuration changes.

Unlike other solutions on the market, Board also supports write-back from cloud to on-premises through a secure tunneling connection. Using this mechanism, data stored in Board can easily be written back to the original source systems within a customer domain.

Board Cloud provides a wide range of connectors to easily integrate different data sources from third-party systems.

The Hybrid Data Pipeline Service supports the data sources shown in the following image:



### 2.3.6 Board Shared Storage (also referred to as Cloud Storage)

In Board Cloud, a Shared Storage Area is provided for importing data into the cloud tenant and exporting data externally. Platforms and sandboxes refer to it as “remote drive Z”. You can leverage it to:

- load files from outside the tenant
- share files between platforms and sandboxes
- store Data Model backups (on-demand or scheduled backups).

The Board Shared Storage is shared across platforms and sandboxes, including storage space and quota. In contrast, local storage refers to the specific and local storage areas within a specific instance, where Board Cloud data and logs reside.

The Board Shared Storage is completely independent between platform and sandbox instances from an infrastructure point of view, with data redundancy in place to increase the reliability of backup restore points.

## 2.4 Board Cloud Pillars of Security

Board Cloud has been built from the ground up in accordance with industry best practices and current regulatory requirements. Board Cloud offers the highest level of security by adhering to the following fundamental concepts:

- **Confidentiality**
- **Integrity**
- **Availability**

Those pillars are guaranteed by the security best practices adopted by Board, which also include the following:

- **Compliance:** due to ISO/IEC 27001, with extensions ISO/IEC 27017 and ISO/IEC 27018 requirements, the Company must respect and ensure the requested confidentiality, availability, and integrity of customer data. Board Cloud is also SOC 1® Type II, SOC 2® Type II, and SOC 3® compliant. Board Cloud is also UNI EN ISO 9001 compliant with a focus on improving efficiency and meeting customer requirements.
- **Business Continuity:** business continuity is guaranteed by Board through Disaster Recovery protocols, Backup Procedures, and Geo Redundancy.
- **Data Retention:** this is necessary for the performance of services, to securely delete all customer data and to offer the needed support to customers during these activities.

## 2.5 Azure Datacenters and Security

Board Cloud is deployed across Microsoft Azure datacenters.

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.

## 2.5.1 Azure Compliance Standards

Board Cloud is deployed across Microsoft Azure datacenters. The list of supported Azure regions and datacenters 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 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 (Azure compliance documentation | Microsoft Learn) (refer to Fig. 1 – Microsoft Azure Regions).

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. Data storage may be limited to a single country, region, or geographical area.

***Fig. 5 – Microsoft Azure Regions***

## 2.5.2 Officially Supported Datacenter Locations

| Country | Region | Location |
|---|---|---|
| Australia | Australia Central | Canberra |
| Australia | Australia East | New South Wales |
| Australia | Australia Southeast | Victoria |
| Brazil | Brazil South | São Paulo |
| Canada | Canada Central | Toronto |
| China | East Asia | Hong Kong |
| France | France Central | Paris |
| Germany | Germany West Central | Frankfurt |
| India | Central India | Pune |
| Ireland | North Europe | Ireland |
| Italy | Italy North | Milan |
| Japan | Japan East | Tokyo |
| Netherlands | West Europe | Netherlands |
| Norway | Norway East | Oslo |
| Singapore | Southeast Asia | Singapore |
| South Africa | South Africa North | Johannesburg |
| Switzerland | Switzerland North | Zürich |
| UK | UK South | London |
| United Arab Emirates | UAE North | Dubai |
| US | Central US | Iowa |
| US | East US | Virginia |
| US | East US 2 | Virginia |
| US | North Central US | Illinois |
| US | South Central US | Texas |
| US | West US | California |

## 2.5.3 IP Addresses and Failover IP Addresses for Allow List

| Region | IP Address | Failover IP Address |
|---|---|---|
| Australia Central | 20.227.162.8 | 20.211.142.167 |
| Australia East | 20.211.142.167 | 20.70.125.83 |
| Australia Southeast | 20.70.125.83 | 20.211.142.167 |
| Brazil South | 191.232.73.50 | 20.118.117.128 |
| Canada Central | 20.104.4.34 | 20.221.44.191 |
| Central India | 20.219.170.112 | 20.197.64.174 |
| Central US | 20.221.44.191 | 20.190.204.137 |
| East Asia | 52.246.138.127 | 20.197.64.174 |
| East US | 20.102.27.66 | 20.245.2.108 |
| East US 2 | 20.190.204.137 | 20.221.44.191 |
| France Central | 20.19.98.87 | 40.127.238.163 |
| Germany West Central | 20.218.206.120 | 20.50.237.135 |
| Italy North | 4.232.180.133 | 20.19.98.87 |
| Japan East | 20.210.34.202 | 52.246.138.127 |
| North Central US | 20.241.100.41 | 20.118.117.128 |
| North Europe | 40.127.238.163 | 20.50.237.135 |
| Norway East | 51.13.17.62 | 20.108.147.172 |
| South Africa North | 20.87.193.251 | 20.203.117.75 |
| South Central US | 20.118.117.128 | 20.241.100.41 |
| Southeast Asia | 20.197.64.174 | 52.246.138.127 |
| Switzerland North | 20.250.135.116 | 20.19.98.87 |
| UAE North | 20.203.117.75 | 20.87.193.251 |
| UK South | 20.108.147.172 | 51.13.17.62 |
| West Europe | 20.50.237.135 | 40.127.238.163 |
| West US | 20.245.2.108 | 20.102.27.66 |
| West US 2 | 52.143.75.156 | 20.221.44.191 |

*The above IP addresses are designated for delivering new Board Cloud Tenants. Existing Board Cloud Tenants will only begin using these IP addresses after receiving a specific notification. If you haven't received this notification, your Tenant will continue to use the previously configured static IP address.

**The IP addresses above are only related to: Subscription Hub portal, Platform portal(s), Sandbox portal(s), and administrator portal(s).

# 3. Cloud Security

## 3.1 Board's User Provisioning (IT Setup)

Once the agreement is signed, Board Cloud initiates the user provisioning process.

After the Cloud Operations team has successfully deployed the Board Cloud customer instance, a series of emails are sent to the authorized customer point-of-contact appointed in the contract.

The provisioning process:

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. A second email is sent to the primary contact of the account with the activation link referenced in step 1. The primary contact, as first user, will be the Subscription Hub administrator and will login as "admin".
3. Once the user clicks the activation link, the user is taken to the Board Subscription Hub where they can create a password for the administrator account.
4. Once the password has been created (step 3), a third email is sent inviting the user to activate the new account. Activate the account by clicking on the activation link included in the email.

The provisioning is complete when the customer completes the activation tasks outlined above.

## 3.2 Single Sign-On (SSO)

Board Cloud supports various authentication methods through the Subscription Hub. Authentication can be configured in two ways:

1. Board user accounts
2. External Identity Providers (IDPs) using industry standard protocols, such as SAML 2.0 and OIDC

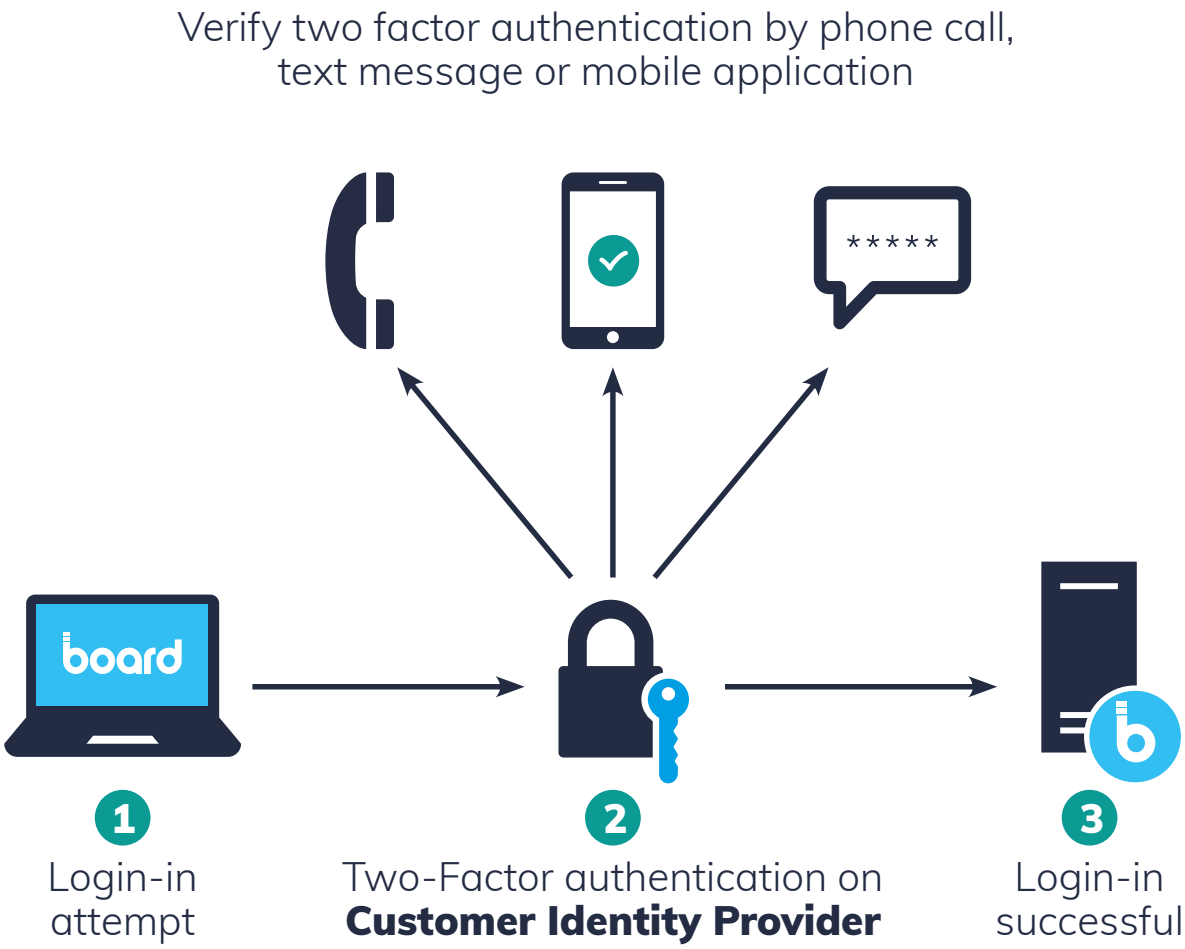
Utilizing external IDPs can simplify deployment, minimize user administration, and improve the user experience of Board Platforms with SSO (Single Sign-On) capabilities, thanks to direct integration with centralized company authentication systems already in use.

This feature also enables customers to directly manage login options, password policies, lockout policies, and other specific settings, right from the Subscription Hub.

Board Cloud implements Federated Authentication using Security Assertion Markup Language (SAML 2.0) or OpenID Connect (OIDC), as illustrated below.

By enabling the authentication to be handled by an OIDC- or SAML 2.0-based Identity Provider, the two-factor authentication can also be implemented, as shown in the diagram below.

*Fig. 6 – Two Factor Authentication*



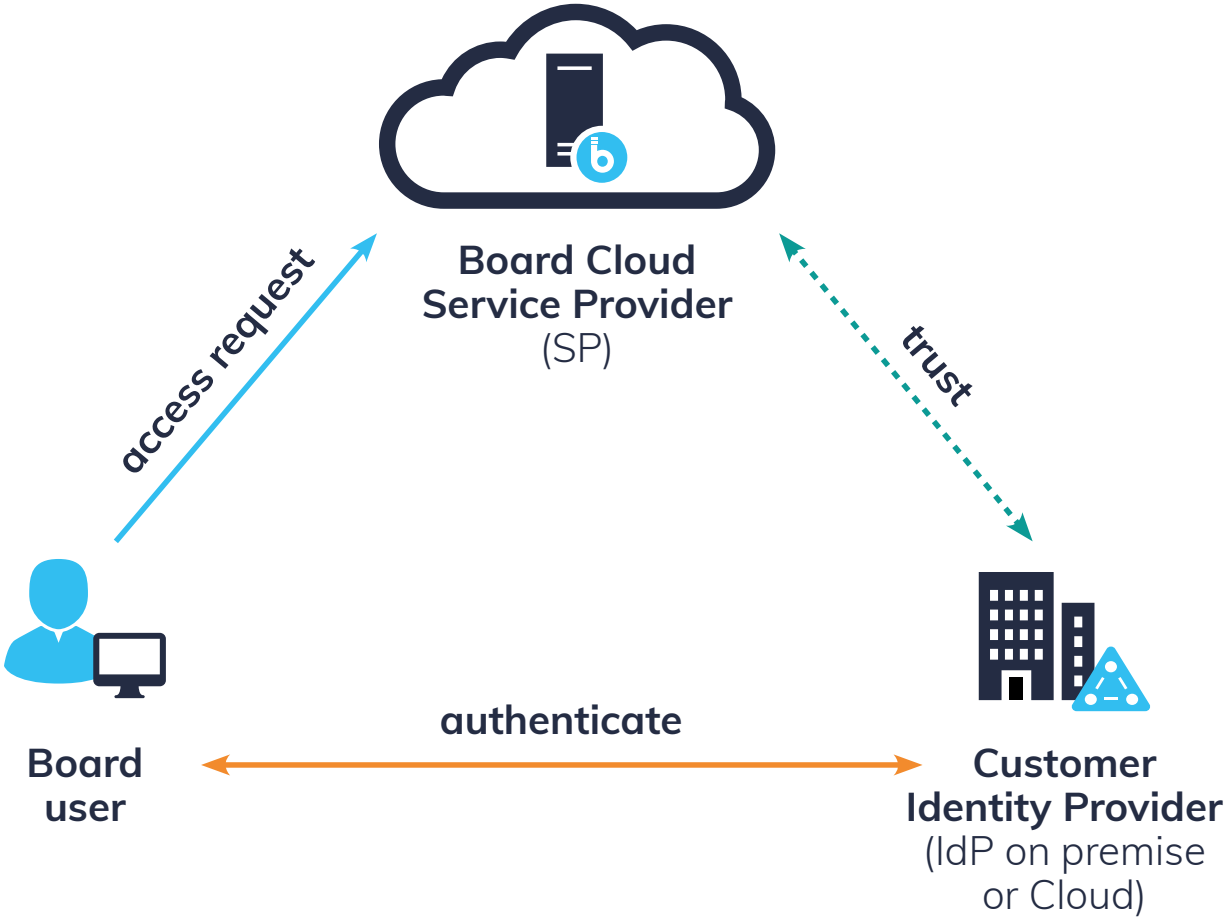

### 3.2.1 Single Sign-On Authentication

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).

***Fig. 7 – Board SSO Architecture***




## 3.3 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 passwords for Board user accounts must meet the following requirements:

- **At least 8 characters**
- **At least 1 uppercase letter, 1 numeric character and 1 special character**
- **Expiration after 365 days**
- **May not repeat one of the last 5 passwords used**
- **5 login attempts: 5 login attempts with the wrong password will disable the account for 30 minutes**.

## 3.4 Audit Logs

Board's extensive logging capability provides customers with a comprehensive 360-degree view of their Board Cloud environment. This is achieved through log files that capture an extensive amount of information, such as all user activity, login/logout/failed login attempts, procedure execution, data entry (before and after values), creation or modification of Screens, and many more.

- All log records are time-stamped and capture user IDs as well as other details typically found in verbose level logging mechanisms.
- All logs can be encrypted and downloaded so that customers can upload and process them in other systems or applications.
- All the logs are kept in a secure, tamper-proof area within the customer's environment.

### 3.4.1 Logs & Auditability

All access is monitored and logged, including any access to the cloud environment by the Board Cloud Operations.

**Customer Logs**

All customer end-user access is also logged and made available to customers 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.

**Log Security**

All log files are securely stored on an Azure repository.

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.

## 3.5 Board Employee Access and Control

Only the Cloud Operations Team can access Board Cloud Resources. This access is only permitted with two-factor Authentication (2FA), and access to any datacenter server and its resources is further protected by an SSL VPN that uses a personal encryption certificate.

Only selected Board employees who signed ad-hoc clauses for administrators have access to customer data file system, for maintenance and operational reasons: all employee access is tracked and frequent audits are performed.

## 3.6 Cyber Controls and Network Architecture

Board utilizes countermeasures, tools, processes, and controls to guarantee the integrity, confidentiality and availability of data and of the service.

## 3.6.1 Physical Security of MS Datacenter

Microsoft datacenters are designed and managed to provide physical control over the areas in which data is stored. Microsoft takes a layered approach to physical security to reduce the risk of unauthorized users having physical access to data and datacenter resources.

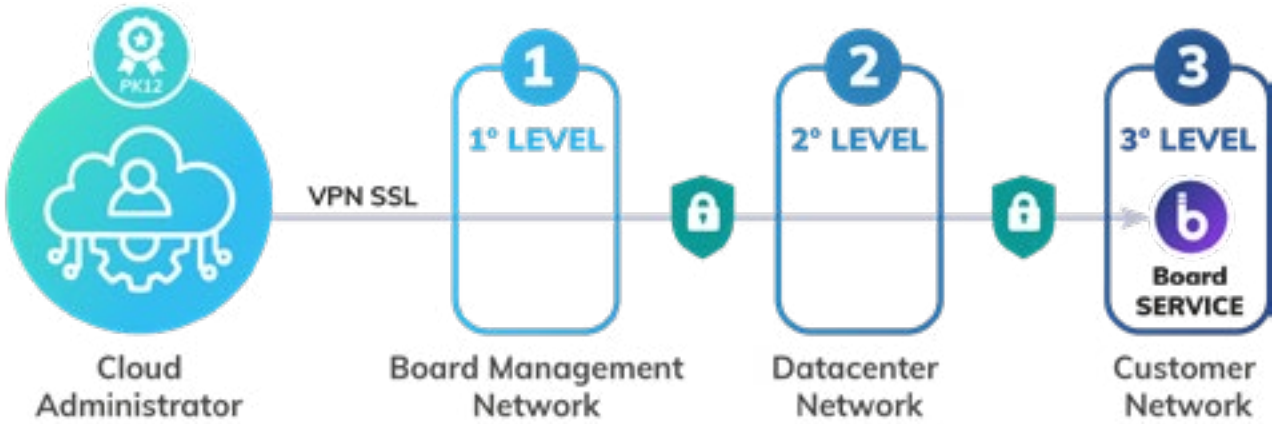
Datacenters have extensive levels of protection such as approval of access to the perimeter of the facility, the perimeter of the building, the inside of the building, and the floor of the datacenter.

Microsoft is an industry leader in setting clear security and privacy requirements, and, therefore, consistently meets those requirements. In fact, Azure complies to a wide range of international and industry-specific certifications of compliance standards.

## 3.6.2 Access Restriction and Network Segregation

The network is segregated on multiple levels. A virtual network is the cornerstone of the Board Cloud networking model and provides isolation and protection.

***Fig. 8 – Access Restriction and Network Segregation****




*Only selected Board employees who signed ad-hoc clauses for administrators have access to customer data file system, for maintenance and operational reasons: all employee access is tracked and frequent audits are performed.

Reverse proxies and WAF are configured at the edge of Board Cloud infrastructure like incoming traffic controllers and support TLS on ingress for secure access. They leverage containerization and are deployed to any adopted Azure region.

## 3.6.3 DDoS Protection

DDoS (Distributed Denial-of-Service) Protection is a standard service that provides enhanced DDoS mitigation capabilities for Board SaaS applications. This includes dedicated monitoring along with machine learning that automatically configures DDoS protection policies.

## 3.6.4 Detection and Response

According to our defense strategy, intrusion detection systems collect signals from either the internet and private networks, turn them into detections, and provide automatic responses or trigger Board internal SOC, a team of security experts that are responsible for monitoring, detecting, and investigating threats and vulnerabilities and, consequently, to improve and enforce Cloud systems.

### 3.6.5 Secure Coding

Secure Coding refers to a set of principles and fundamentals that guide the developer to write safe code, introducing a first line of defense against potential security risks. The basics of good security practices are:

- Access control, which includes authentication and authorization
- Enforcing strong cryptography, according to standard algorithms

Board has adopted a multi-layer security approach, adhering to the defense-in-depth principle. This strategy involves building a secure software development lifecycle (SDLC) and integrating secure programming practices and code quality into the software development process. Applications are created and maintained at every stage, from initial requirements gathering to development, testing, deployment, and maintenance. Additionally, Board has implemented a secure coding initiative, utilizing automated and interactive tools to periodically perform Static Application Security Testing (SAST), Software Composition Analysis (SCA), and Dynamic Application Security Testing (DAST) on the source code and its platform.

### 3.6.6 Antivirus/Anti-Malware Protection

Implemented defense layers help to identify and remove viruses, spyware, and other malicious software. Anti-malware provides configurable alerts when known malicious or unwanted software attempts to install itself or run on the system.

### 3.6.7 Software Development Lifecycle Assurance

Based on Agile system development methodology, the software development lifecycle assurance analysis in addition to its design, development, test, and deployment phases allow users to determine, apply, and test countermeasures for the possible threats detected for each feature developed. For additional details, please see the document: "Board_Cloud_Development_LifeCycle_and_Release_Strategy".

### 3.6.8 Change Management

The organization has specific procedures for the efficient and timely management of all changes as well as for the control of the IT infrastructure, in order to minimize the number and impact of any service-related incidents.

### 3.6.9 Cloud Control Room

The monitoring system supervises the system's health by analyzing system events such as network capacity, hardware performance/failure, and cyber-attacks. The resources are monitored 24/7.

# 3.7 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:

- Defining adequate management structure to prepare, mitigate, and respond to adverse events. This is made effective and impactful by a defense and protection system capable of applying corrective actions and promptly engaging the SOC team
- Appointing suitable personnel to respond to incidents with the necessary responsibility, authority, and competence to handle an accident and maintain the security of information
- Developing and approving 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.

Each event requires further investigation by the SOC team to classify the alert and then take appropriate actions based on the scenario, following a specific remediation plan.

Upon the conclusion of each event, a detailed incident report is always created, outlining all necessary information for a clear understanding of the event. Additionally, potential improvements to systems, resources, and policies are identified and studied.

In accordance with the SaaS agreement, Board will notify the customer of any ongoing incident within the specified timeframe.

In the event of an incident requiring investigation (e.g., security breaches or legal inquiries), Board will take reasonable steps to preserve relevant digital evidence, including:

- activity logs, system logs, and audit trails
- access records
- backup data and other pertinent records.

This evidence will be securely retained to prevent alteration, destruction, or loss during the investigation or as legally required. If Board receives a request for information (e.g., court orders or regulatory inquiries) related to Customer Data or Board SaaS Services, it will:

- notify the Customer, unless legally prohibited, allowing them to contest or seek protective measures
- disclose evidence only as required by law and limit the disclosure to the minimum necessary.

# 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 customer data.

Cloud Operations team members do not have access to customer data, except in the following two scenarios:

1. **With the prior written consent of the customer, to respond to system or technical problems**
2. **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 and Isolation

Board Cloud secures data both in transit and at rest using strong encryption algorithms.

Data at rest is encrypted through AES 256-bit encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. All backups of customer information are also encrypted.

Data in transit is protected with at least TLS 1.2 using a 2048-bit RSA certificate with SHA256.

Board SaaS also supports BYOK, which further increases confidentiality at the application server layer. Keys and certificates are saved in vaults within the tenant and inherit isolation.

Customer Data and records are protected through access controls, encryption, and secure storage solutions. Retention policies ensure that data is preserved as required and securely disposed of when no longer needed.

### 4.3.1 Bring Your Own Key Encryption (BYOK)

The customer can also decide to encrypt logs and data in each Data Model using personal keys (BYOK).

## 4.4 Risk Assessment & Management

Board performs a continuous assessment of the security posture of cloud workloads and receives recommendations from threat intelligence solution and partners for reducing exposure.

By regularly monitoring dashboards and analyzing potential impact of reported vulnerabilities on infrastructure, according to well-known MITRE CVE frameworks, Board is able to prioritize security operations and remediations.

Additionally, Board performs regular tests and hacking simulations on its SaaS to find gaps in security. Board also values customers who report their own tests and strives to help those with strict requirements meet their internal policies, when possible.

By doing so, Board capitalizes on these opportunities to enhance security measures and ensure alignment with industry standards.

Board has established procedures and documentation to ensure that penetration tests are conducted securely and in accordance with relevant guidelines:

- Board Group Internal Procedure: how to manage customer's Penetration Test request
- Board Customer Engagement Rules Penetration Test

### 4.4.1 Board Software Development Life Cycle

Board incorporates security during the software development lifecycle. Board has and follows an Agile system development methodology composed of four 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 the new code containing 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.

### 4.4.2 Vulnerability Testing

Board has a process of vulnerability assessment/penetration testing in place to detect vulnerabilities, which is performed by an independent third party highly specialized in cybersecurity.

This test is carried out at least once a year in addition to each major release.

## 4.4.3 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 version |
| **Medium** | 4.0 – 6.9 | 180 days | Latest version |
| **High** | 7.0 – 8.9 | 90 days | Latest version & all supported versions |
| **Critical** | 9.0 – 10.0 | 30 days | Latest version & all supported versions |

* Rating is established based on the current version of the Common Vulnerability Scoring System (CVSS) 4

In case of a zero-day 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.

## 4.4.4 Certifications

Board has obtained the following certifications and accreditations for its Board Cloud service:

**ISO/IEC Certifications**

The scope of the following certifications is "design and development of the Board platform for Business Intelligence, Performance management and Analytics, and its own installation, maintenance, and support through Cloud SaaS (Software as a Service), using the ISO/IEC 27017:2015 and ISO/IEC 27018:2019 guidelines."

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems – Requirements
- ISO/IEC 27017:2015 Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- ISO/IEC 27018:2019 Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

**UNI/EN ISO Certification**

The scope of the following certification is "design and development of the Board platform for Business Intelligence, Performance management and Analytics, and its own installation, maintenance, and support through cloud SaaS (Software as a Service)."

- UNI/EN ISO 9001:2015 Quality management systems

Organizational and technical security measures are implemented and annually audited.

## 4.4.5 System & Organization Controls

Board is regularly audited by a third party to assess the controls and processes in place to address the risks associated with an outsourced service. Board has obtained System and Organization Controls (SOC), SOC 1®, SOC 2®, and SOC 3® compliance reports.

# 5. Integrated Quality and Information Security Management Systems

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, in addition to monitoring information security ongoingly.

Moreover, Board has implemented an Integrated Quality and Information Security Management System (IMS) in accordance with UNI EN ISO 9001:2015, ISO/IEC 27001:2022, ISO/IEC 27017:2015, and ISO/IEC 27018:2019 with the aim to:

- improve the performance of business processes and results
- guarantee the protection of confidentiality, integrity and availability of its information assets, including customer information and personal data
- achieve and improve the satisfaction of customers and other stakeholders in accordance with the objectives set by Management.

This system contains policies, procedures, guidelines, work instructions, and checklists for internal use and is distributed to all employees. The information security officer (ISO) regularly reviews and updates security policies. This review assesses the availability, confidentiality and integrity of information resources, as well as compliance with the information security policy.

## 5.1 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:

### 5.1.1 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 it 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.

### 5.1.2 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, as well as 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 security and availability controls.

The SOC 2 Type II report includes a detailed description of the tests and 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.

### 5.1.3 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 and can be downloaded from the URL: https://www.board.com/en/governance-and-compliance

### 5.1.4 ISO/IEC 27001:2022, ISO/IEC 27017:2015, and ISO/IEC 27018:2019

Board maintains ISO/IEC 27001:2022, ISO/IEC 27017:2015, and ISO/IEC 27018:2019 certifications for Board Cloud to demonstrate its conformity with the defined requirements in these standards.

Jointly published by the International Standard Organization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27001:2022, ISO/IEC 27017:2015, and ISO/IEC 27018:2019 are globally recognized information security standards that provides organizations with requirements for an Information Security Management System (ISMS).

ISO/IEC 27017 provides additional guidelines for information security controls applicable to cloud services, enhancing the security of cloud environments and ISO/IEC 27018 focuses on the protection of personally identifiable information (PII) in public clouds, ensuring privacy and data protection.

An annual audit is conducted to validate compliance with the standards, and a full certification occurs every three years. Board's ISO/IEC certificates are available for customer and prospective review.

The scope of certifications is the following: **"Design and development of 'Board' platform for Business Intelligence, Performance management and Analytics and its own installation, maintenance, supporting through cloud SaaS service. (Software as a Service), using the ISO/IEC 27017:2015 and ISO/IEC 27018:2019 guidelines."**

### 5.1.5 UNI EN ISO 9001:2015

Board maintains UNI EN ISO 9001:2015 certification for Board Cloud demonstrating its commitment to quality management principles.

An annual audit is conducted to validate compliance with the standards, and a full certification occurs every three years. Board's ISO/IEC certificates are available for customer and prospective review. The scope of certifications is the following: "Design and development of "Board"; platform for Business Intelligence, Performance management and Analytics and its own installation, maintenance, supporting through cloud SaaS service. (Software as a Service)"

## 5.2 Cloud Security Alliance

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to ensure a secure cloud computing environment.

As a CSA member, Board International has completed the Cloud Security Alliance (CSA) STAR Level 1: STAR Registry Listing for Board Cloud | CSA (cloudsecurityalliance.org)

## 5.3 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:

- Defining adequate management structure to prepare, mitigate, and respond to adverse events.
- Appointing suitable personnel to respond to incidents with the necessary responsibility, authority, and competence to handle an accident and maintain the security of information.
- Developing and approving 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.

# 6. Cloud Reliability & 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 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 prevent data loss through the backup/restore strategies.
- **System event:** controls and procedures that guarantee service continuity and restoration in case of failure.
- **Procedure and policy:** 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 and hardware performance/failure.

## 6.1 Business Impact Analysis (BIA)

Business continuity is guaranteed through a series of measures, such as the adoption of technologies, tools, and processes to manage any disasters in the shortest possible time, ensuring that the service is always available and working in any type of situation.

In order to identify and apply all countermeasures aimed at eliminating or reducing potential threats to business continuity and to ensure the highest level of security and integrity, Board has conducted a Business Impact Analysis (BIA) and a risk assessment following a standardized and structured methodological approach.

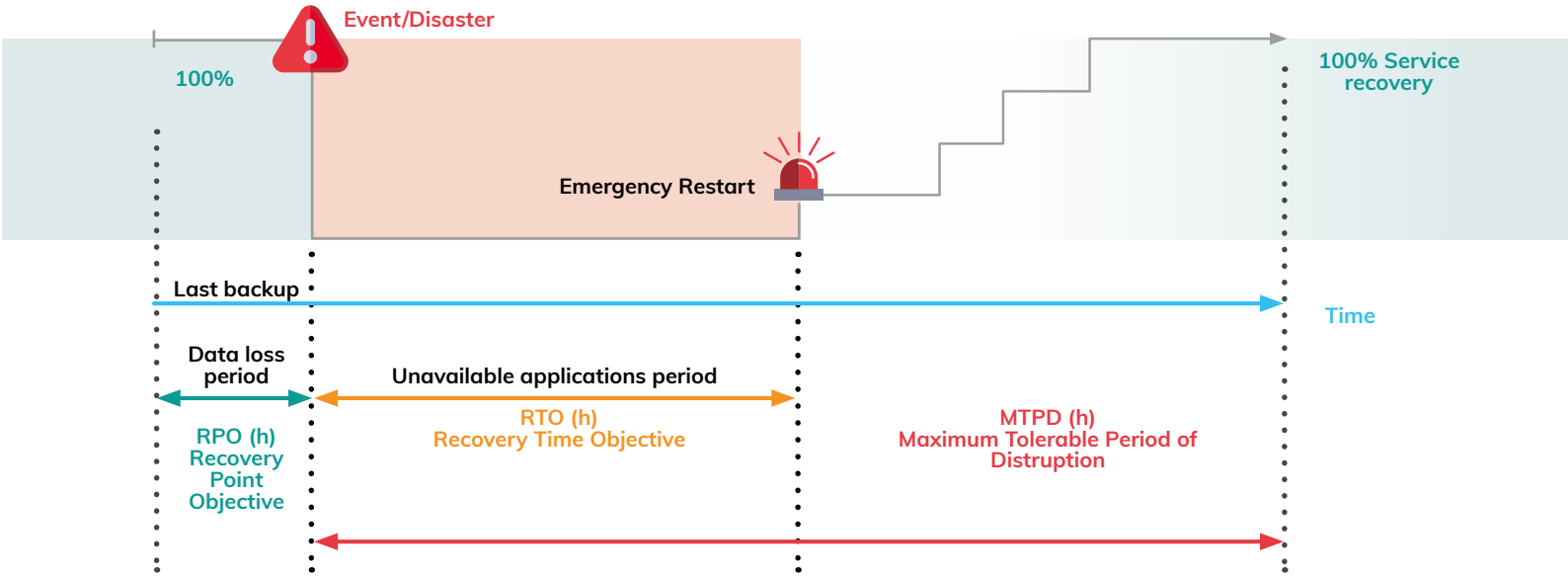
This enables the identification of services that are vital for keeping the SaaS service running and available even in the case of catastrophic and unexpected events.

### 6.1.1 Methodological Approach

The methodological approach followed for the creation of the Business Continuity plan is:

1. Estimate and validate:
    a. the BIA perimeter and, consequently, the processes (and related services) involved
    b. risk (crisis) scenarios
    c. timescales
    d. the financial impact ranges of undesirable events
    e. the financial impacts for each process/service involved
    f. MTPD (maximum time potential damage), RTO (recovery time objective), RPO (recovery point objective) for each process/service involved
2. Identify and map critical assets and critical resources related to each process.
3. Consequently identify, among all business processes and services, the critical ones together with their MTPD, RTO, and RPO.
4. Identify MTPD, RTO, and RPO for each resource related to critical business processes and services.

*Fig. 9 – Diagram RPO, RTO, and MTPD*




RTO and RPO numerical values are shown in the Board SaaS agreement.

On the basis of the results of the BIA and the risk assessment, Board has defined and managed the operational continuity (in a Business Continuity plan) of the business processes identified as critical.

## In particular, Board has:

1. created a process for the evaluation of events aimed at analyzing and identifying their nature using best practices and reference standards. Specifically, the collection of events, subsequent impact assessments, categorization, and the related diagnoses is expected.

**The two main categories of the event considered in business continuity are:**

a. incidents

b. crises

**Based on nature, two different processes are triggered:**

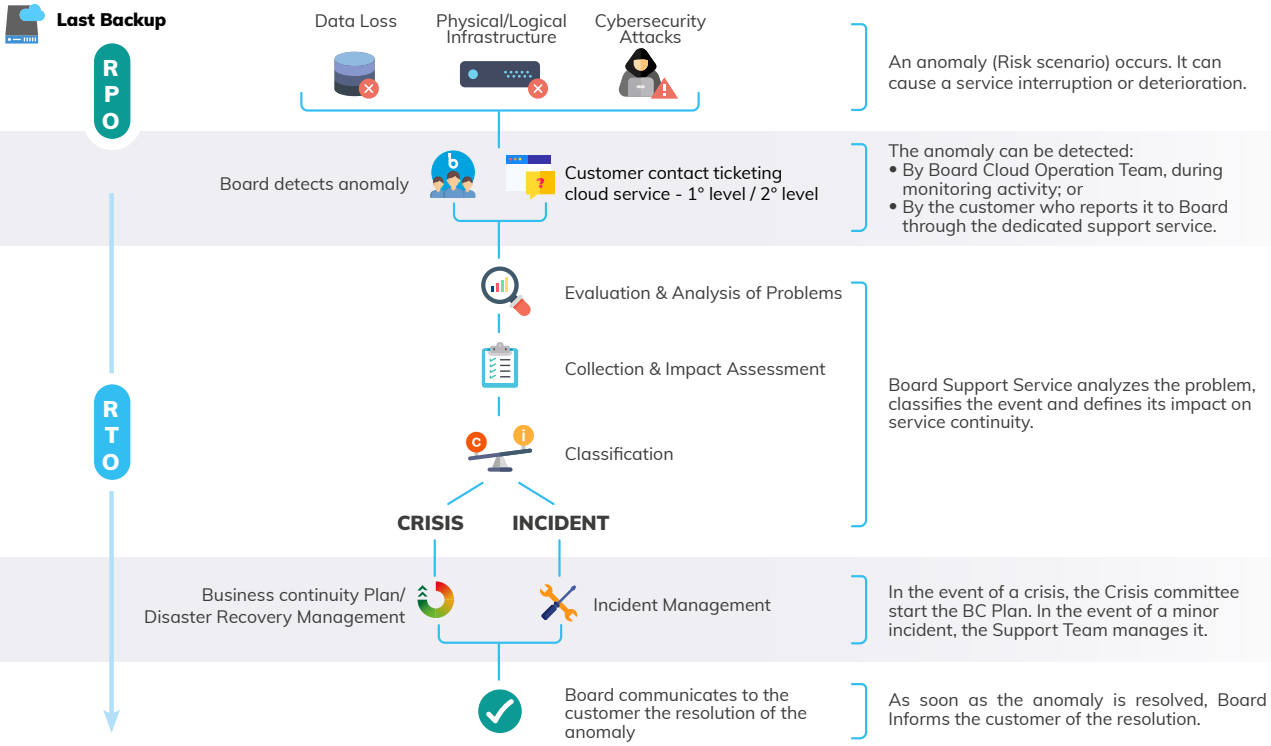
c. In the event of an incident, an incident management process is carried out, followed by the support team.

d. In the event of a crisis, an evaluation is performed by the crisis committee and the relevant disaster recovery process is activated.

2. applied and strengthened a series of security countermeasures within the ISO 27001 Management System perimeter.

Hereafter, you will find a representation of the business continuity process in the case of several risk scenarios.

*Fig. 10 – Flow chart of business continuity process following some risk scenario examples*




The whole process is implemented to ensure the service's recovery according to the Board SaaS agreement.

## 6.2 Business Continuity Measures

Board's methodological approach to business continuity management requires the BIA and risk assessment activities referred to in the previous paragraph. In order to deal with possible crisis scenarios and manage them if they arise, Board applies preventive countermeasures aimed at ensuring continuity and security.

### 6.2.1 Redundancy & High Availability

Board operates with a fully redundant cloud infrastructure that guarantees the availability, robustness, high reliability, and resilience of the internal cloud service.

The redundancy, in particular, is ensured by the presence of different layers that allow, on one hand, the management of failover, ensuring high-level performance of the infrastructure, and on the other hand, the maintenance of high- level security and reliance.

## 6.2.2 Datacenter Redundancy

Board uses Azure datacenters to take advantage of high availability, disaster recovery and backup on Azure's global network. Azure safeguards data in facilities that are protected by industry-leading physical security systems and comply with a comprehensive portfolio of standards and regulations.

Azure has more global regions than any other cloud provider, which provides the scale needed to bring applications closer to users worldwide, preserving data residency and offering customers comprehensive compliance and resiliency options. The Azure network can handle failures and respond quickly to peak demand. To support the enormous growth of cloud services and maintain a consistent level of performance, Microsoft invests in private fiber for metropolitan, land, and submarine routes. Microsoft owns and operates one of the largest backbone networks in the world, connecting Azure datacenters and customers (please refer to ***Figure 11*** below).

***Fig. 11 – Global physical networking paths between datacenters***


## 6.2.3 Data Redundancy

Board's officially supported Azure regions ensure data redundancy by using availability zones or paired regions in the same geography.

Azure availability zones are designed to provide high availability and disaster recovery. Within an Azure region, Azure guarantees that availability zones are separated far enough from one another to ensure that a failure in one zone does not affect the others, each with independent power, cooling, and networking.

Each region has multiple availability zones, which are made up of multiple datacenters far enough apart to protect applications from datacenter-level failures, such as power outages, floods, or fires, but close enough to provide low-latency connections.

Customer data located on the dedicated encrypted storage accounts is continuously replicated to ensure durability and high availability. The in-place replications create copies of data to protect from planned and unplanned events, including but not limited to transient hardware failures, network or power outages, and massive natural disasters. Data is constantly maintained with at least two healthy replicas.

In addition, system restore points of every customer environment are geographically replicated to guarantee cross-regional disaster recovery.

## 6.2.4 Datacenter Redundancy Compliance

Board Cloud is deployed exclusively on Microsoft Azure datacenters around the world.

All datacenters comply with key industry standards, such as ISO/IEC 27001:2022 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 datacenters allows Board to:

1. 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.
2. choose a datacenter in proximity to the customer's user base.

## 6.2.5 Board Service Redundancy Policies and Controls

Each customer has a dedicated environment which includes a pool of computing resources and storage areas.

Redundancy and availability of the resources pool is guaranteed through a multi-layer redundant architecture. All data associated with Disaster Recovery (customer data, configuration data, and environment settings are necessary to restore the full service) is organized over two layers, configured by default as follows:

**1. Datacenter Layer**

All infrastructure data, as in environment configurations, settings, and resource 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 two types of retention policies, explained in the following section under Data backups.

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

## 6.2.6 Data Backups

Automated and full data backups are performed for each Board environment once a day with the following retention policy:

- last 15 days rolling with a snapshot of the entire environment.
- last 3 months rolling with a snapshot of the entire environment taken on the first day of the month.

The daily backups policy described above is intended solely for disaster recovery purposes and not available to the end users. Customers should perform their own backups using Board's self-service backup feature to fulfill their data protection policy according with their applications and business use cases lifecycles.

## 6.2.7 Disaster Recovery Plan Test

Board performs annual BCDRP Tests, Business Continuity, and Disaster Recovery Plan tests. The procedure steps of the Board's Business Continuity Plan (including the Disaster Recovery Plan) determine whether the plan and the test meet the Recovery Time Objective ("RTO") and the Recovery Point Objective ("RPO") expectations, and they help ensure personnel knowledge about recovery process and incident management during disaster recovery.

The annual disaster recovery plan test (DRP test) includes a cross-regional restoration of a Board Cloud instance and Subscription Hub in the secondary disaster recovery region.

## 6.2.8 Board Service Management & Service Teams Continuity

The continuity of the business and of the service offered to the customers is granted by the availability and expertise of the cloud team that manages the cloud services.

The Cloud Operations Team is the only department that can access Board Cloud resources. This access is only permitted with Two Factor Authentication (2FA), and access to any server in the datacenter is further protected by an SSL VPN that uses a personal encryption certificate. Thanks to this security enforcement, access to Cloud resources is possible from anywhere and through any device.

The Ticketing Service is accessible from multiple locations in order to guarantee service in the event of the unavailability of an office and/or its infrastructure.

## 6.3 Shared Responsibility Model

The following table shows the roles and responsibilities for guaranteeing the continuity of vital components of the service, deriving from the business impact analysis.

| Actors | Board International | Customer |
|---|---|---|
| **Component** | ✓ | |
| Data Center Redundancy | ✓ | |
| Physical Infrastructure countermeasures | ✓ | |
| Board tenant Service Redundancy | ✓ | |
| Board tenant Service Backups | ✓ | |
| Customer application Business Continuity* | | ✓ |
| Customer application Data Backups** | | ✓ |
| Application level security measures*** | | ✓ |
| Customer Data Encryption | ✓ | |
| SaaS Cyber-attack countermeasures | ✓ | |

*Customer applications developed by the customer (Board Data Models, Capsules, and Procedures) should be designed and implemented in accordance with best practices, considering the business continuity requirements of the application (i.e. the customer is responsible for testing changes to the Data Model and Capsules before deployment into production).

** The customer is required to manage their own applications' data and perform data backups

*** The application security layer is designed and developed by the customer during the implementation. The customer is responsible for:

- granting new user access and ascertaining that terminated employees have no access to the System, revoked in a timely manner
- ascertaining that written process instructions for the administration of authorizations exist and include responsibilities, authorization instructions, and authorization administration
- regularly reviewing the user profiles and the access activities associated to the accounts
- guaranteeing, by all actors involved, timely intervention in case anomalies occur in their areas of responsibility.

# 7. The People of Board

## 7.1 Information Security Roles

Board is composed of technical departments staffed by people highly specialized in security and business continuity. The key figures/teams responsible for the continuity and reliability of the service offered and the ability to meet customer needs are as follows:

- Software Development Team, to safely develop new features for the Board Platform.
- Cloud Operations Team, to ensure the efficient and effective daily monitoring and control of the Platform.
- Security Incident Management Group, to manage all anomalies to safeguard the security and availability of the service and analyze these anomalies to understand and identify if there is any reason to declare a crisis.
- Information Security Manager, to regularly review and update security policies by assessing the availability, confidentiality, and integrity of data and to update the Business Continuity Management System.
- Crisis Committee, to assess whether an abnormal condition should be declared a crisis, in order to activate the business continuity plan.

### 7.1.1 Support Service

Board provides and guarantees a technical support service that deals with the incident management process. It is composed of highly specialized personnel with linguistic and geographical coverage available 24/7.

The team is organized according to common ITIL incident management practices. Failure events can be identified, reported, and managed in a timely manner. In this way, Board guarantees the restoration of normal service functions in the shortest possible time, minimizing the potential negative impacts of adverse events. Additionally, Board has a strong and effective user community where experts contribute by sharing knowledge, skills, and experience.

## 7.2 Board Employee Security Training

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.

Board ensures the validation of references and the appropriate level of background checks. For Board, it is crucial to increase the level of expertise and to raise awareness to ensure that law, guidelines, and procedures relating to information security are in full compliance.

Board has various initiatives in place 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 a minimum of 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 need 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).**

## 7.2.1 Team Competencies and Training

Board's technical staff is subjected to a formal screening process that includes a required background check before joining the team.

Typically, the team's ability to face potential disaster situations is evaluated. Knowledge, experience, skill level, and attitude are examined on the basis of previous work responsibilities or participation in real disasters.

All team members are extensively trained in cloud security and operational procedures, while operational activities are periodically audited. Procedures and rules are regularly reviewed and updated in order to guarantee a continuous improvement principle.

The Board Cloud staff excel in multi-tasking and ensure the development of best-practice techniques for managing projects/programs in their daily activities. Cloud Team members have years of industry experience in addition to well-known industry certifications, such as CCSP.

# 8. Glossary

**BC/Business continuity**
Capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incidents.

**BCP/Business continuity plan**
Documented procedures that guide the organization to respond, recover, resume, and restore to a pre-defined level of operation following disruption.

**Client**
A device used to access Board.

**Crisis**
An occurrence and/or perception that threatens the operations, staff, shareholder value, stakeholders, brand, reputation, trust, and/or strategic/business goals of an organization.

**DRP/Disaster recovery plan**
Documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.

**Incident**
A situation that might be, or could lead to, a disruption, loss, emergency, or crisis.

**Instance**
Any customer-specific Platform or Sandbox environment where users can connect and work. An instance is connected to the Subscription Hub, to have centralized user and administration management across multiple instances.

**MTPD/Maximum tolerable period of disruption**
The maximum time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, before becoming unacceptable.

**Penetration test**
Testing or ethical hacking is the practice of testing a computer system, network, or web application to find security vulnerabilities that an attacker could exploit.

**Platform**
A customer-specific instance, connected to Subscription Hub, used as a production environment.

**RPO/Recovery point objective**
Point to which information used by an activity must be restored to enable the activity to operate on resumption.

**RTO/Recovery time objective**
Period of time following an incident in which product or service must be resumed, or activity must be resumed, or resources must be recovered.

**Sandbox**
A customer-specific instance, connected to the Subscription Hub, used as a pre-production, development, and testing environment.

**Tenant**
A customer-specific group of resources which includes all instances and the Subscription Hub.

**VPN/Virtual private network**
Technology that creates a safe and encrypted connection over a less secure network, such as the internet.

**Vulnerability assessment**
Process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

**Zero-day vulnerability**
An unknown flaw in the security software identified by the mitigator, such as a developer or security team.

EN2503U

www.board.com