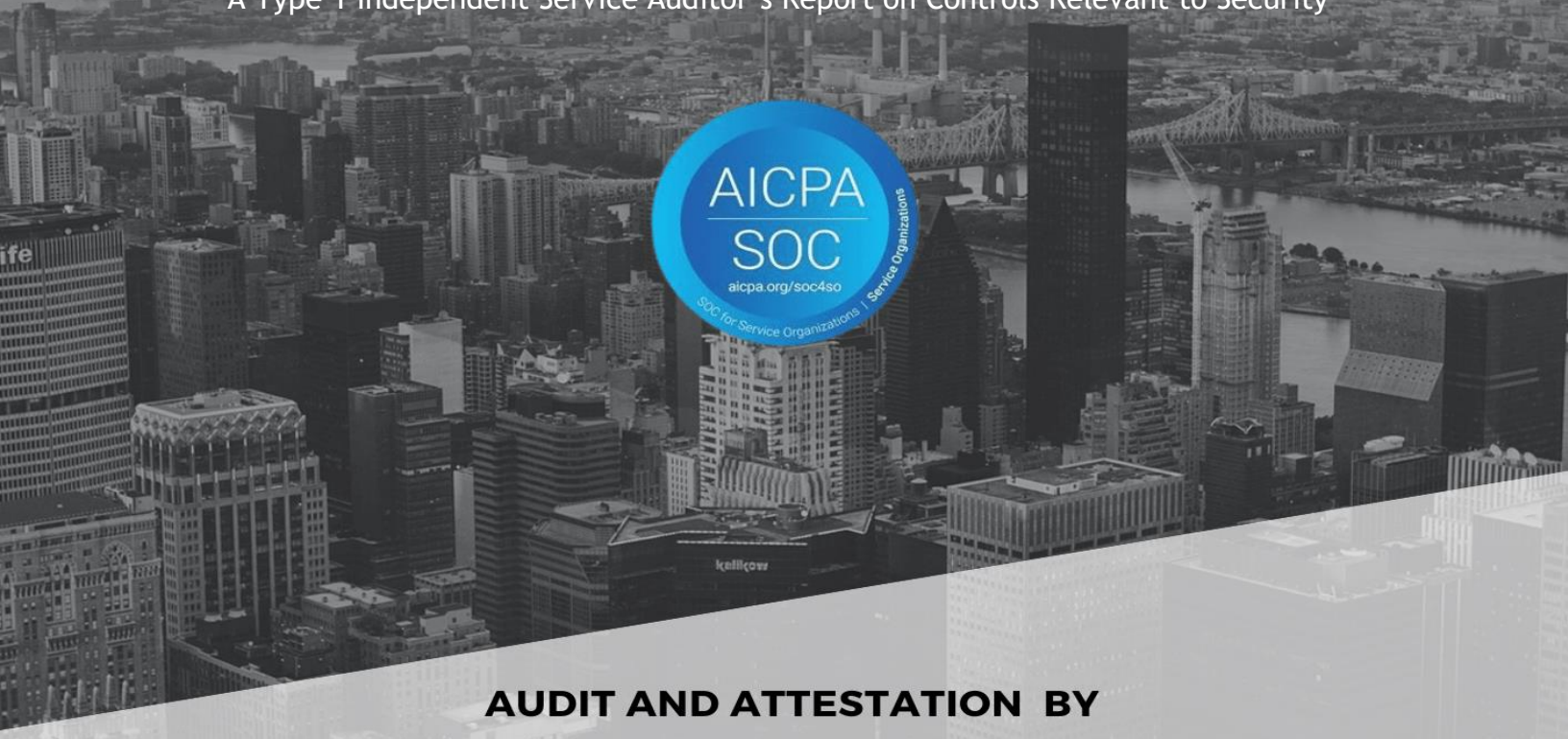
SOC 2 Type 1 Report

IntelliBoard Pro

August 28, 2023

A Type 1 Independent Service Auditor's Report on Controls Relevant to Security



AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

CPA

Prescient Assurance LLC.
1100 Market Street Suite 600
Chattanooga, TN 37402

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319

Table of Contents

SECTION 1

Management's Assertion

Management's Assertion

We have prepared the accompanying description of IntelliBoard Pro's system as of May 4, 2023, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report. The description is intended to provide report users with information about IntelliBoard Pro's system that may be useful when assessing the risks arising from interactions with IntelliBoard Pro's system, particularly information about system controls that IntelliBoard Pro has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

IntelliBoard Pro uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at IntelliBoard Pro, to achieve IntelliBoard Pro's service commitments and system requirements based on the applicable trust services criteria. The description presents IntelliBoard Pro's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of IntelliBoard Pro's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at IntelliBoard Pro, to achieve IntelliBoard Pro's service commitments and system requirements based on the applicable trust services criteria. The description presents IntelliBoard Pro's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of IntelliBoard Pro's controls.

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

A. The description presents IntelliBoard Pro's system that was designed as of May 4, 2023, in accordance with the description criteria.
B. The controls stated in the description were suitably designed as of May 4, 2023, to provide reasonable assurance that IntelliBoard Pro's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of IntelliBoard Pro's controls as of that date.

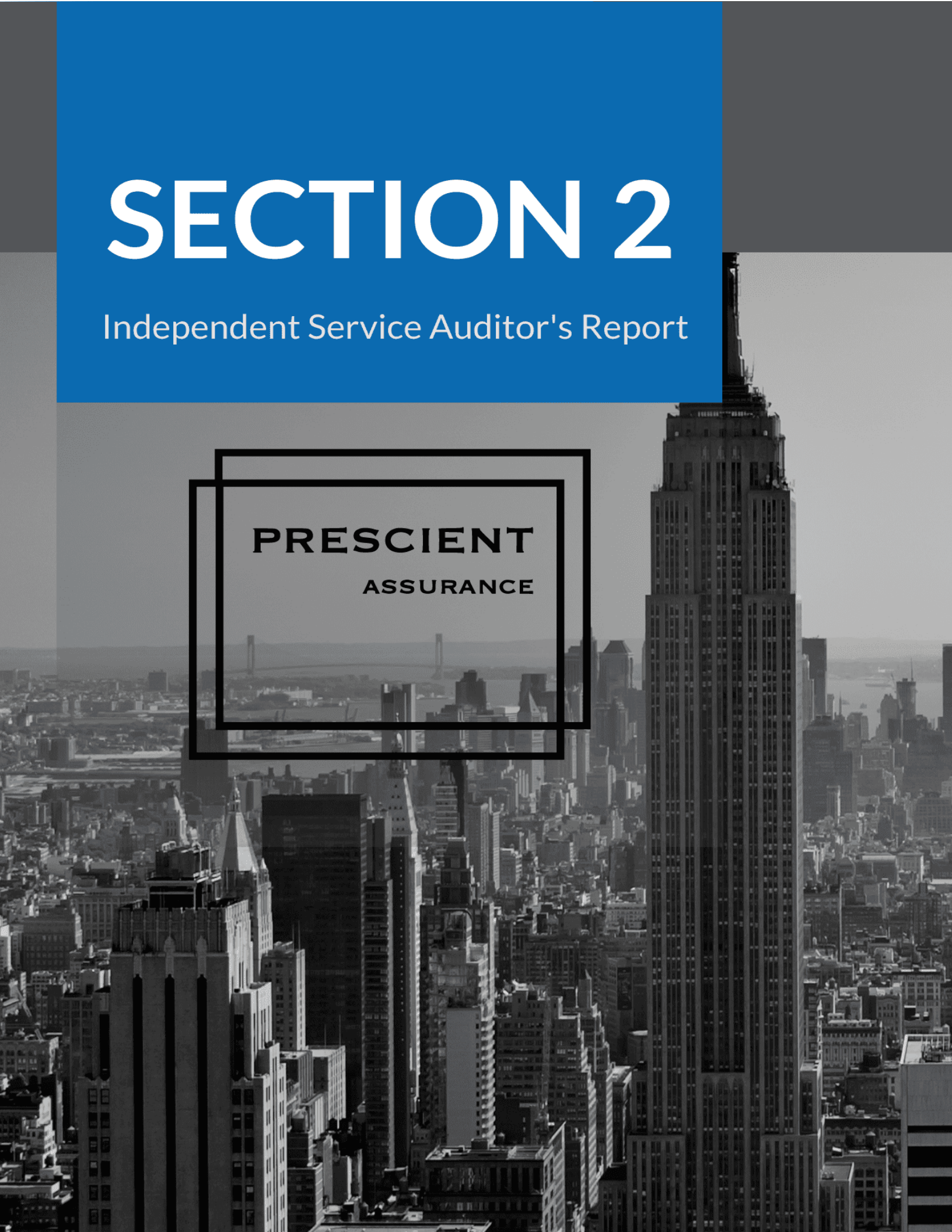
DocuSigned by:
199E7483262F473...

Tonya Riney

Chief Operating Officer of IntelliBoard Pro

SECTION 2

Independent Service Auditor's Report



Independent Service Auditor's Report

To: IntelliBoard Pro

Scope

We have examined IntelliBoard Pro's ("IntelliBoard Pro") accompanying description of its system as of May 4, 2023, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, and the suitability of the design of controls stated in the description as of May 4, 2023, to provide reasonable assurance that IntelliBoard Pro's service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

IntelliBoard Pro uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at IntelliBoard Pro, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents IntelliBoard Pro's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of IntelliBoard Pro's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at IntelliBoard Pro, to achieve IntelliBoard Pro's service commitments and system requirements based on the applicable trust services criteria. The description presents IntelliBoard Pro's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of IntelliBoard Pro's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design of such controls.

Service Organization's Responsibilities

IntelliBoard Pro is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that IntelliBoard Pro's service commitments and system requirements were achieved. In Section 1, IntelliBoard Pro has provided the accompanying assertion titled "Management's Assertion of IntelliBoard Pro" (assertion) about the description and the suitability of design of controls stated therein. IntelliBoard Pro is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

1. Obtaining an understanding of the system and the service organization's service commitments and system requirements.
2. Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
4. Performing procedures to obtain evidence about whether controls stated in the description were suitably designed and implemented to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
5. Evaluating the overall presentation of the description.

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects:

A. The description presents IntelliBoard Pro's system that was designed as of May 4, 2023 in accordance with the description criteria.
B. The controls stated in the description were suitably designed as of May 4, 2023, to provide reasonable assurance that IntelliBoard Pro's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of IntelliBoard Pro's controls as of that date.

Restricted Use

This report is intended solely for the information and use of IntelliBoard Pro, user entities of IntelliBoard Pro's system as of May 4, 2023, business partners of IntelliBoard Pro subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

1. The nature of the service provided by the service organization.
2. How the service organization's system interacts with user entities, business partners, and other parties.
3. Internal control and its limitations.
4. Complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
6. The applicable trust services criteria.
7. The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Prescient Assurance LLC

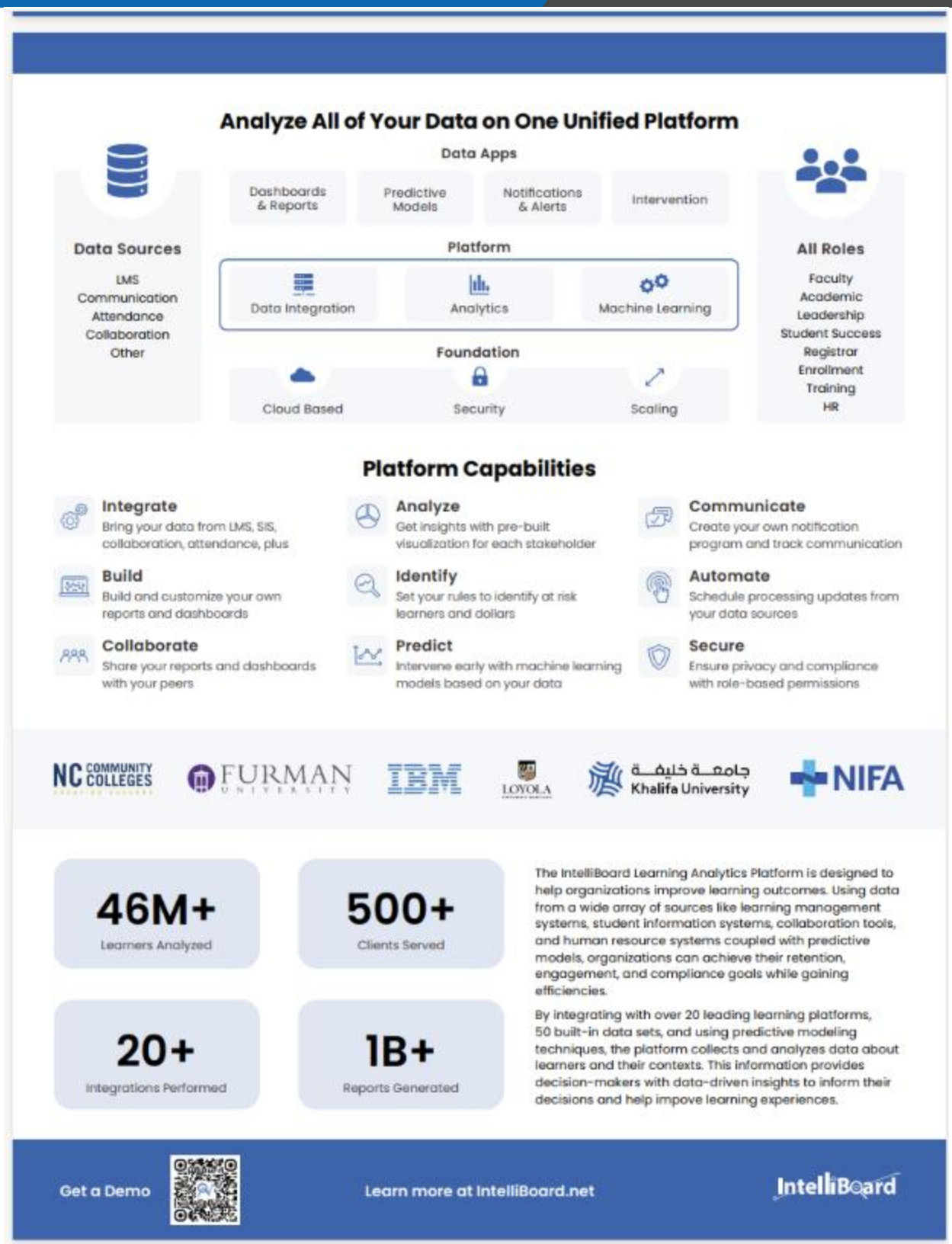
DocuSigned by:
John D Wallace
F5ADFA3569EA450...

John D. Wallace, CPA
Chattanooga, TN
August 28, 2023

SECTION 3

System Description

DC 1: Company overview and types of products and services provided


Analyze All of Your Data on One Unified Platform
Data Apps
Dashboards & Reports
Predictive Models
Notifications & Alerts
Intervention
Data Sources
LMS
Communication
Attendance
Collaboration
Other
Platform
Data Integration
Analytics
Machine Learning
Foundation
Cloud Based
Security
Scaling
All Roles
Faculty
Academic
Leadership
Student Success
Registrar
Enrollment
Training
HR
Platform Capabilities
Integrate
Bring your data from LMS, SIS, collaboration, attendance, plus
Analyze
Get insights with pre-built visualization for each stakeholder
Communicate
Create your own notification program and track communication
Build
Build and customize your own reports and dashboards
Identify
Set your rules to identify at risk learners and dollars
Automate
Schedule processing updates from your data sources
Collaborate
Share your reports and dashboards with your peers
Predict
Intervene early with machine learning models based on your data
Secure
Ensure privacy and compliance with role-based permissions
NC COMMUNITY COLLEGES
FURMAN UNIVERSITY
IBM
LOYOLA
جامعة خليفة
Khalifa University
NIFA
46M+
Learners Analyzed
500+
Clients Served
20+
Integrations Performed
1B+
Reports Generated
The IntelliBoard Learning Analytics Platform is designed to help organizations improve learning outcomes. Using data from a wide array of sources like learning management systems, student information systems, collaboration tools, and human resource systems coupled with predictive models, organizations can achieve their retention, engagement, and compliance goals while gaining efficiencies.
By integrating with over 20 leading learning platforms, 50 built-in data sets, and using predictive modeling techniques, the platform collects and analyzes data about learners and their contexts. This information provides decision-makers with data-driven insights to inform their decisions and help impove learning experiences.
Get a Demo
Learn more at IntelliBoard.net
IntelliBoard

DC 2: The principal service commitments and system requirements

Response Times	Initial Response	Ongoing Response
Severity 1	1-2 hours	1 day
Severity 2	1-5 hours	1-3 days
Severity 3	1-5 hours	7-14 days (sprint metrics)
Severity 4	1-5 hours	7-14 days (sprint metrics)

Severity 1: A problem that severely impacts your use of the software in a production environment (such as loss of production data or in which your production systems are not functioning). The situation halts your business operations and no procedural workaround exists.

Severity 2: A problem where the software is functioning but your use in a production environment is severely reduced. The situation is causing a high impact to portions of your business operations and no procedural workaround exists.

Severity 3: A problem that involves partial, non-critical loss of use of the software in a production environment or development environment. For production environments, there is a medium-to-low impact on your business, but your business continues to function, including by using a procedural workaround. For development environments, where the situation is causing your project to no longer continue or migrate into production.

Severity 4: A general usage question, reporting of a documentation error, or recommendation for a future product enhancement or modification. For production environments, there is low-to-no impact on your business or the performance or functionality of your system. For development environments, there is a medium-to-low impact on your business, but your business continues to function, including by using a procedural workaround.

Data Processing Addendum

IntelliBoard Pro's Data Processing Addendum (DPA) is organized into parts, depending on the type of access IntelliBoard Pro will have. Part A applies to all third-party service providers. Part B applies, in addition to Part A, to the extent IntelliBoard Pro accesses, supports, manages or stores Information Systems that contain IntelliBoard Pro Protected Data and that are owned and/or controlled by IntelliBoard Pro in order to carry out its responsibilities under the Agreement. Part C applies, in addition to Parts A and B, to the extent IntelliBoard Pro accesses, supports, manages, or stores IntelliBoard Pro Protected Data using Information Systems that are outside IntelliBoard Pro's span of control in order to carry out IntelliBoard Pro's responsibilities under the agreement.

Part A

1. **Acknowledgement.** The parties acknowledge and agree that any disclosure of Protected Data, will in no way be construed to be an assignment, transfer, or conveyance of title to or ownership rights in such Protected Data.
2. **Compliance.** Customers will provide Protected Data to IntelliBoard Pro as reasonably required for IntelliBoard Pro to comply with its responsibilities under the Agreement. The nature and purpose of Processing and the type of Personal Data provided may be further described in the Agreement. Personal Data provided to IntelliBoard Pro may include Personal Data of the following categories of natural persons: Customer employees, students, independent

contractors, agents, vendors, suppliers, customers or prospective customers or individuals employed by or that interact with Customer employees or students.

3. **Purposing.** IntelliBoard Pro will Process Personal Data only to the extent required for IntelliBoard Pro to carry out its responsibilities under the Agreements, and IntelliBoard Pro will not retain, use, or disclose Personal Data for any purpose other than for the specific purpose of performing the services specified in the Agreement. IntelliBoard Pro will not sell, rent, disclose, disseminate, make available, transfer, or otherwise communicate Personal Data to another business or third-party for monetary or other valuable consideration.
4. **Processing per Instruction.** IntelliBoard Pro shall comply with instructions provided by Customer during the term of the Agreement regarding Protected Data and shall only Process Protected Data in accordance with such instructions.
5. **Reporting Harmful Activity.** IntelliBoard Pro shall promptly report activity that may reasonably lead to physical harm to individuals, loss of information (including, but not limited to Personal Data) or damage to facilities or equipment to Customer.
6. **Unplanned Event Procedures.** IntelliBoard Pro will implement and regularly evaluate a procedure to provide for continuation of business operations during unplanned, adverse events.
7. **Response to Inquiries.** IntelliBoard Pro will assist Customer in responding to requests from individuals related to Personal Data about them. In the event that IntelliBoard Pro receives a request from an individual regarding Personal Data provided to IntelliBoard Pro by Customer, IntelliBoard Pro will promptly notify Customer of such request and will not respond to such request without the prior written consent of Customer's Data Protection Officer, except where required by applicable law.
8. **Obligational Compliance.** IntelliBoard Pro will assist Customer to comply with Customer's obligations to perform data protection impact assessments.
9. **Use of Third-Parties.** IntelliBoard Pro will not transfer or otherwise make available Personal Data to any third-party (including a subcontractor or law enforcement agency) without the prior written consent of Customer's Data Protection Officer, except as required by applicable law. IntelliBoard Pro will not transfer or permit the transfer of Personal Data to any employee, student, agent, or subcontractor for any reason with first entering into a written agreement containing terms requiring that party to abide by substantially similar restrictions and conditions that apply to IntelliBoard Pro in this DPA. Customer acknowledges and agrees that, subject to the terms of this DPA, the subcontractors listed in Attachment 1 may be used for the Processing of Personal Data. In the event that IntelliBoard Pro receives a request or demand for Personal Data by a law enforcement or other governmental agency, IntelliBoard Pro will, except where prohibited from doing so by applicable law, direct the agency to Customer and promptly notify Customer of the request or demand.
10. **Information Security Program.** IntelliBoard Pro will designate an Information Security Officer to be responsible for the information Security program. Such individual will respond to Customer inquiries regarding computer security. The information security program will be modeled after the requirements of NIST, SOC II, ISO 27001 and other globally recognized information security standards and will be compliant with all applicable legal and regulatory requirements for data protection and privacy of Protected Data. Without limiting IntelliBoard Pro's obligation of confidentiality in the Agreement and as further described herein, IntelliBoard Pro will be responsible for establishing and maintaining an information security program that is designed to
    1. ensure the security and confidentiality of Protected Data

2. protect against any anticipated threats or hazards to the security of integrity of the Protected Data
3. protect against unauthorized access to or use of the Protected Data
4. ensure the proper disposal of Protected Data as further defined herein and
5. ensure that all subcontractors of IntelliBoard Pro who have access to Customer's Protected Data or access to Customer's Information Systems used to Process Customer Protected Data, if any, are approved by Customer and comply with all of the foregoing. IntelliBoard Pro will designate an individual to be responsible for the information security program.

11. **Compliance, Right to Audit, and Incident Notification.** IntelliBoard Pro will promptly, and without undue delay, notify the designated Customer security contact in writing of any security incidents as described below. The notice shall include the approximate date and time of the occurrence and a summary of the relevant facts, including a description of measures being taken to address the occurrence. IntelliBoard Pro will promptly respond to requests for information from Customer related to any actual or suspected security incidents. A "security incident" includes and unauthorized access to Customer's Information Systems or Protected Data; access, unauthorized or unplanned disruption of service due to malicious actor(s), or unauthorized modification of systems or data. Upon thirty (30) days prior written Notice, Customer or its third-party designee may request to view the results of audits and/or compliance records of the IntelliBoard Pro environment that may include, but are not limited to, review of documentation, as they relate to the receipt, maintenance, use, retention, and authorized destruction of Customer information, including Protected Data. Any applicable regulator shall have the same right upon request. IntelliBoard Pro shall promptly provide all information reasonably requested by Customer to determine IntelliBoard Pro's compliance with the terms of this DPA and shall provide reasonable assistance to Customer or its regulators or agents upon thirty (30) days prior written Notice. IntelliBoard Pro agrees to comply with legal requirements that are identified during such audits within reasonable timeframes. Customer reserves the right to view, upon request, assessment reports that IntelliBoard Pro has undertaken on its behalf to assess IntelliBoard Pro's own network security. IntelliBoard Pro will provide its full cooperation and support regarding any notices required by applicable law to individuals who may be adversely affected by a security incident.
12. **IntelliBoard Pro Data Handling Procedures.** Protected Data must be physically and logically secured when not in use and securely disposed of upon Customer's request or the termination or expiration of the agreement. Destruction of Protected Data on electronic media shall be according to Section 13 below. Destruction of Protected Data on paper shall be by shredding by IntelliBoard Pro or a third-party that provides secure document destruction services. Upon request, IntelliBoard Pro will provide information to Customer regarding procedures for secure destruction of Protected Data.
13. **Erasure of Information and Destruction of Electronic Storage Media.** All electronic storage media containing Protected Data must be wiped or degaussed for physical destruction or disposal in a manner meeting forensic industry standards such as the NIST SP800-88 Guidelines for Media Sanitization or other methods authorized by Customer. IntelliBoard Pro must maintain documented evidence of data erasure and destruction. This evidence must be available for review at the request of Customer.
14. **Personnel Screening.** IntelliBoard Pro will not assign any person to the Agreement who has not been screened, or whose screening according to the standards has revealed that the person does not meet standards. Where such checks are prohibited by applicable law, IntelliBoard Pro will notify Customer in advance that a particular individual has not been screened under this Section prior to that individual performing work for Customer. If IntelliBoard Pro contracts, for

any services, with a third-party that needs permission or requires access to Protected Data, the third-party will undergo the same screening as performed on IntelliBoard Pro personnel and contractors. IntelliBoard Pro will perform screening on all IntelliBoard Pro personnel and contractors including temporary and non-employee personnel who will have access to Protected Data or directly support such access or the environment storing or Processing that Protected Data during work they perform for Customer pursuant to the Agreement that includes criminal background checks, employment, and education verification, according to the following standards:

1. Criminal Background Investigation from a certified national agency based within the employee's country of origin and/or residence
2. Employment Verification within the past 5 years or previous 3 employers
3. Education Verification the highest level of education attained by an applicant from the specified university.

15. **Personal Data Received from the European Economic Area ("EEA"): Standard Contractual Clauses**
    1. IntelliBoard Pro acknowledges that it may receive Personal Data regarding individuals who are located in the EEA (currently comprising the European Member States, Iceland, Liechtenstein and Norway), Switzerland or the United Kingdom.
    2. IntelliBoard Pro and Customer agree to the terms set forth in the Standard Contractual Clauses (the "Clauses") executed by the parties, attached as Attachment 2 hereto and incorporated herein by reference, to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals. The terms of this DPA shall not replace any comparable or additional rights and obligations relating to Processing Personal Data contained in the Agreement except to the extent such rights or obligations conflict with the terms herein, in which case the terms herein shall control only to the extent such terms conflict.

Part B

1. **Training.** IntelliBoard Pro must conduct formal security awareness training for all personnel and contractors as soon as reasonably practicable after the time of hiring or prior to being appointed who work on Personal Data and annually recertified thereafter. Documentation of Security Awareness Training must be retained by IntelliBoard Pro, confirming that this training and subsequent annual recertification have been completed, and available for review by IntelliBoard Pro.
2. **Network and Communications Security.**
    1. All IntelliBoard Pro connectivity to Customer Information Systems shall be through remote access mechanisms approved by Customer.
    2. IntelliBoard Pro will not transmit any unencrypted Protected Data over the internet and will not store any Personal Data or Restricted Information on any mobile device, except where there is a business necessity and then only if the mobile computing device is protected by industry-standard encryption software or other safeguards approved by Customer. Notwithstanding the foregoing, it is acceptable to transmit the sub-set of Personal Data that consists only of business contact details for individuals involved in the business relationship without using encryption.
    3. IntelliBoard Pro will not access and will not permit unauthorized persons or entities to access, Customer computing systems and/or networks without Customer's express written

authorization and any such actual or attempted access will be consistent with any such authorization.

4. IntelliBoard Pro will take appropriate measures to ensure that IntelliBoard Pro's systems connecting to Customer's systems, and anything provided to Customer through such systems does not contain any malicious code designed to, or that would enable, the disruption, modification, deletion, damage, deactivation, disabling, harm or otherwise be an impediment to the operation of Customer's systems, and IntelliBoard Pro will promptly notify Customer of any material vulnerabilities that could impact Customer.

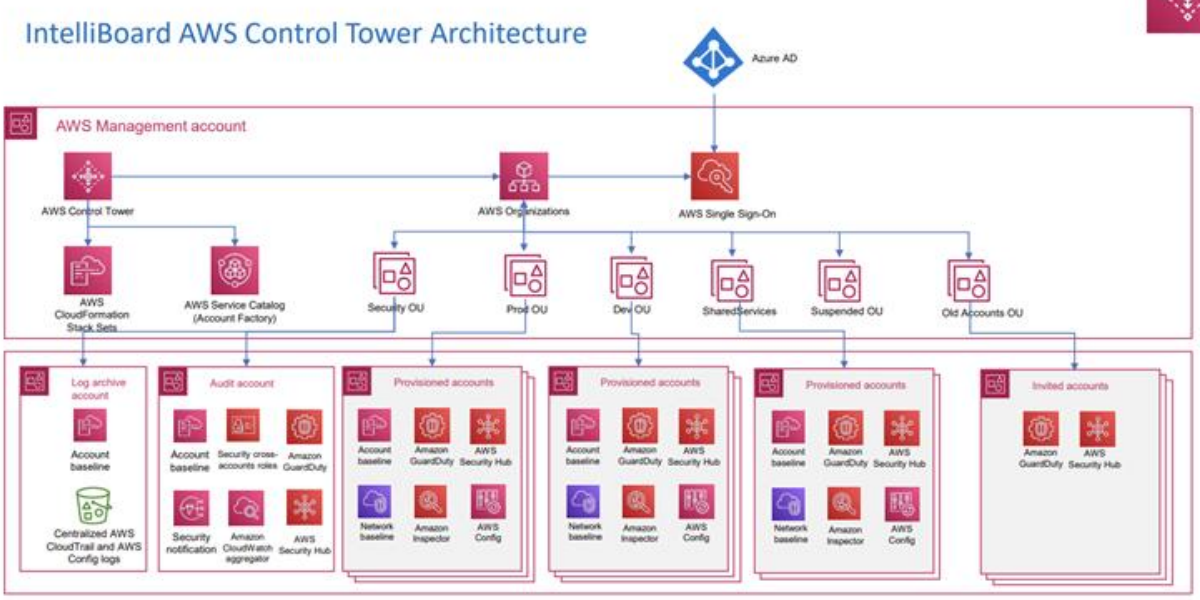
3. **Physical Security**. All Protected Data must be contained in secure, environmentally controlled storage areas owned, operated, or contracted for by IntelliBoard Pro. All Personal Data or Restricted Information must be encrypted in storage and in transit, provided, however, that it is acceptable to transmit the sub-set of Personal Data that consists only of business contact details for individuals involved in the business relationship without using encryption.

Part C

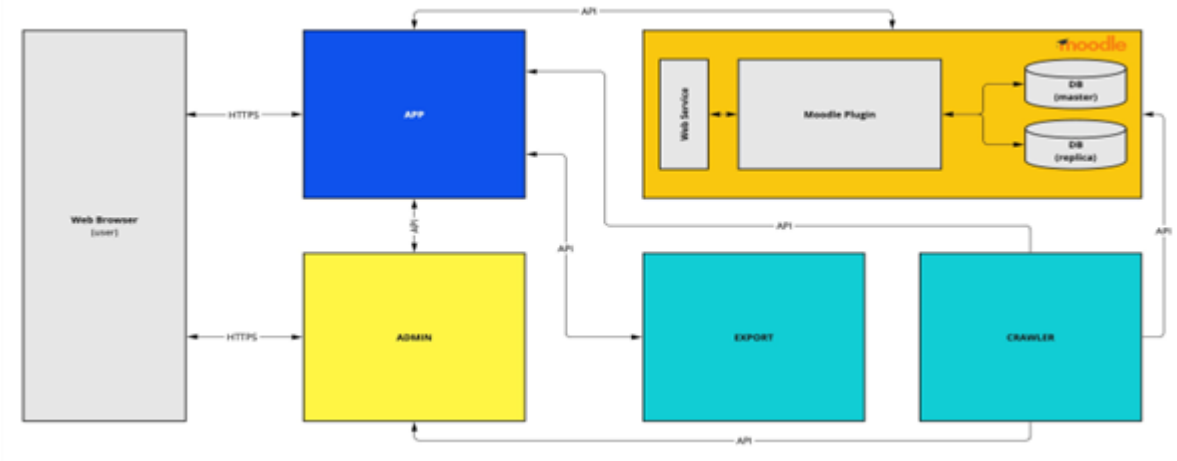
Penetration Testing. During IntelliBoard Pro's performance under the Agreement, IntelliBoard Pro will engage, at its own expense and at least one time per year, a reputable third-party vendor to perform penetration and vulnerability testing ("Penetration Tests") with respect to IntelliBoard Pro's systems containing and/or storing Personal Data or Restricted Information. Within a reasonable period after the annual Penetration Test has been performed, IntelliBoard Pro will notify Customer in writing of any critical level security issues that were revealed during such Penetration Test and subsequently certify in writing to Customer that such critical level security issues have been fully remediated.

DC 3: The components of the system used to provide the services

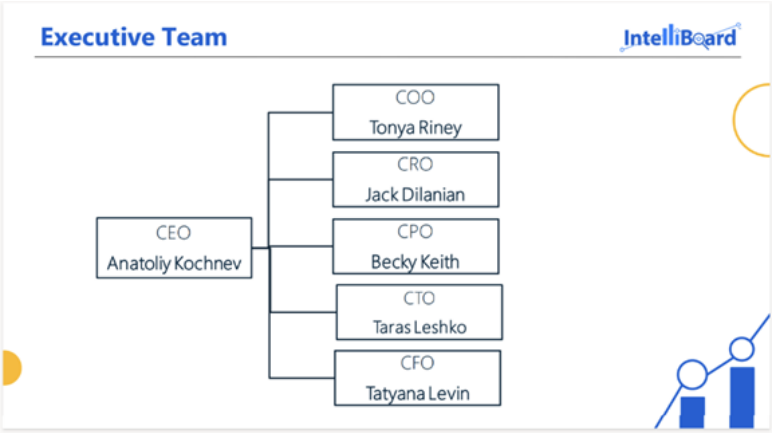
3.1 Primary Infrastructure:

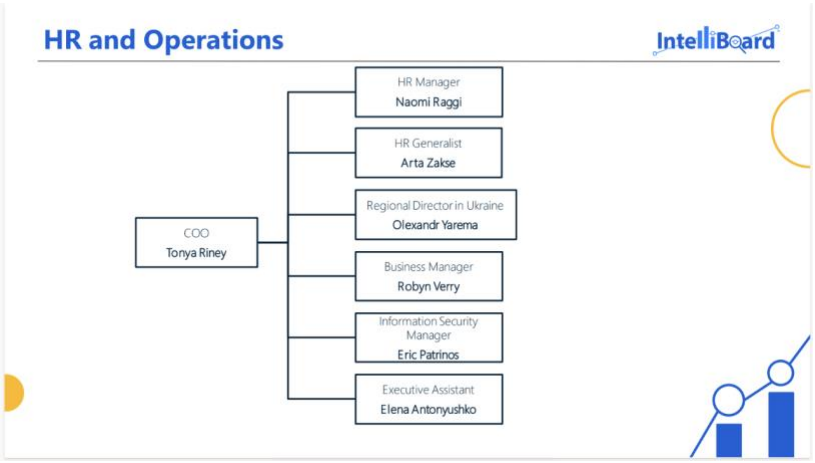


3.2 Primary Software:



3.3 People:





CEO: Overall company leadership and vision.
COO: Execution and development of vision; oversight of HR, Business, and InfoSec
CPO: Execution and development of platform/product(s); oversight of Implementation and Client Success
CRO: Sales leadership, strategy and execution; oversight of Sales, marketing and business development
CTO: Development of technology initiatives, direction and planning for platform/product; oversight of servers and development teams.
InfoSec Manager: Implementation and documentation of strategic information security processes and procedures.
Controller: Oversight of financial management.
Business Office: Administration of business systems (CRM, Project Management), creation and update of PnL, collections.

3.4 Security Processes and Procedures:

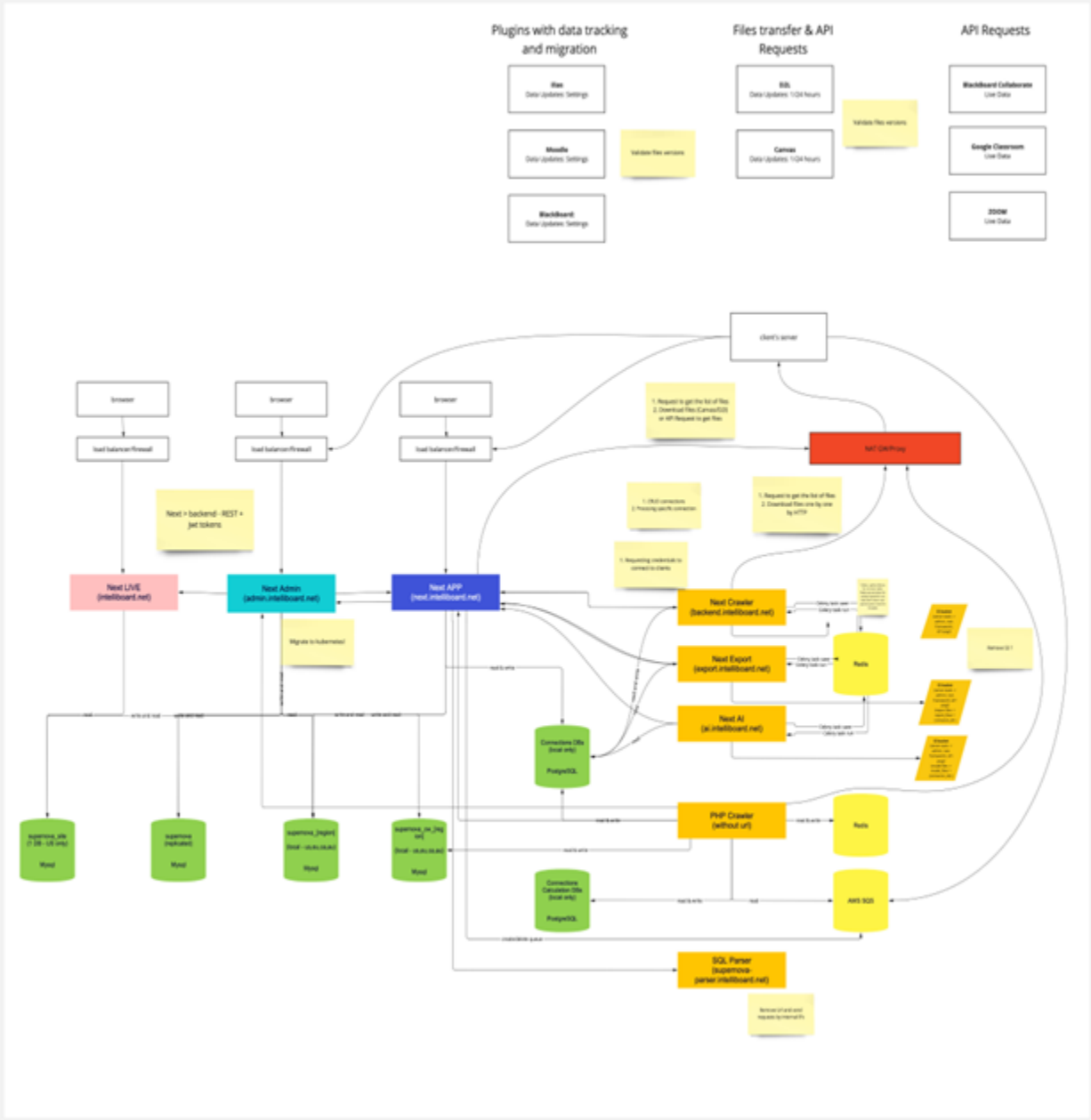
IntelliBoard Pro's Information Security Policy has a purpose to communicate information security policies and outline the acceptable use and protection of IntelliBoard Pro's information and assets. These rules are in place to protect customers, employees, and IntelliBoard Pro. Inappropriate use exposes IntelliBoard Pro to risks including virus attacks, compromise of network systems and services, financial and reputational risk, and legal and compliance issues.

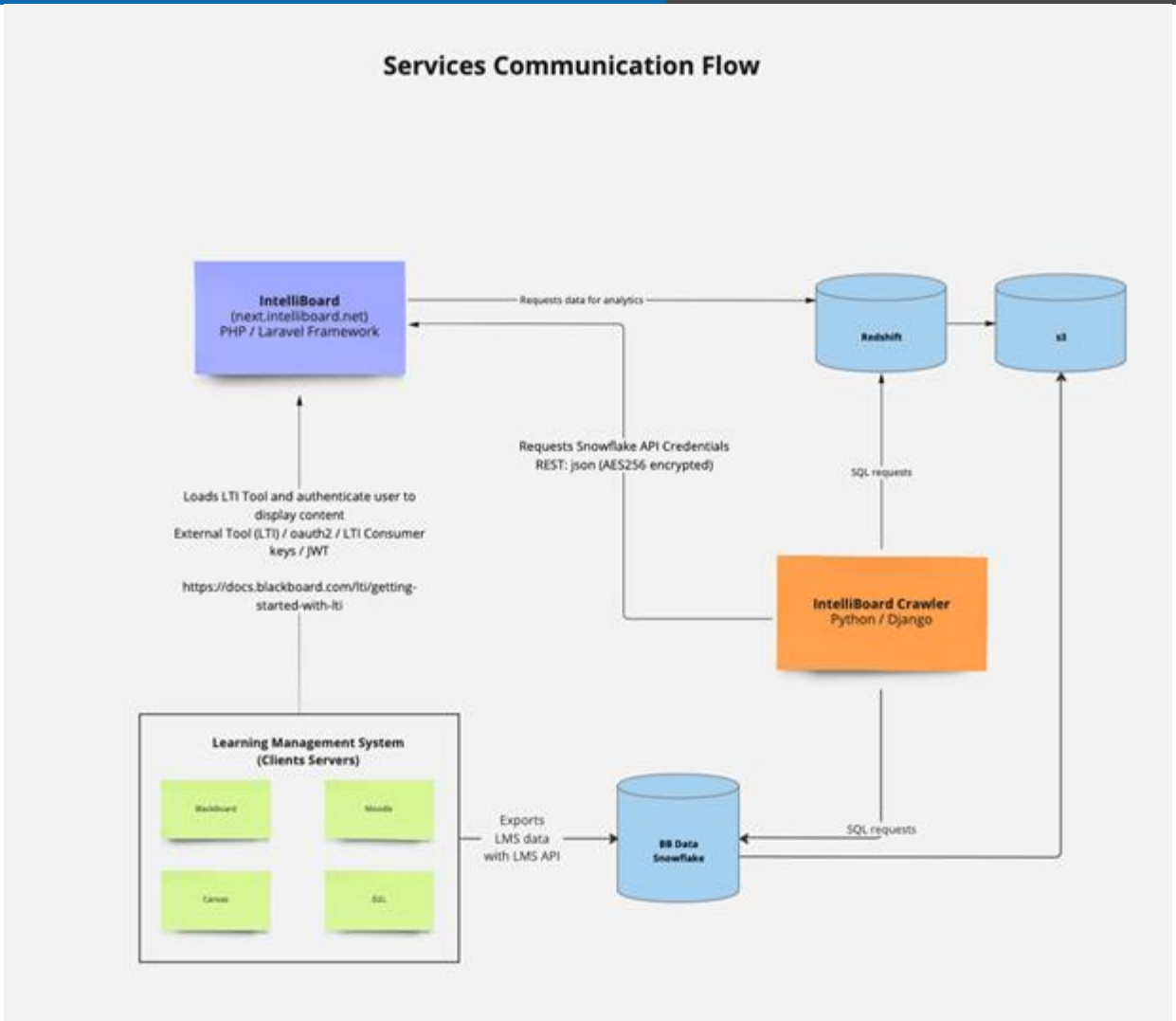
The purpose of the Information Security Policy is to ensure that company employees have as flexible and efficient workflows as possible while ensuring the confidentiality, integrity, and availability of information in our organization and in the services, we provide to our customers.

The Information Security Policy also consists of secure processes and procedures regarding the following topics:

- Information Classification
- Access to Information
- Service Usage of Confidential Data
- Declassification of Data
- Bring Your Own Device (BYOD)
- Removable Media
- Dealing with Secret Information
- Passwords
- Internal and Approved External Services
- Malware Protection and Updates
- Acceptable Use Policy
- Unacceptable Use
- Email and Communication Activities

3.5 Data:


Plugins with data tracking and migration
Files transfer & API Requests
API Requests
Next LIVE (intelliboard.net)
Next Admin (admin.intelliboard.net)
Next APP (next.intelliboard.net)
Next Crawler (backend.intelliboard.net)
Next Export (export.intelliboard.net)
Next AI (ai.intelliboard.net)
PHP Crawler (without url)
SQL Parser (supernova-parser.intelliboard.net)



3.6 Third Party Access:

IBPro is utilized through Amazon Web Services (AWS) cloud-based solution. This is where the product stores, processes, and transmits sensitive data.

3.7 System Boundaries: (Product lines/ LOBs/ brands)

The IntelliBoard Pro Learning Analytics Platform is designed to help organizations improve learning outcomes. Using data from a wide array of sources like learning management systems, student information systems, collaboration tools, and human resource systems coupled with predictive models, organizations can achieve their retention, engagement, and compliance goals all while gaining efficiencies.

By integrating with over 20 leading learning platforms, including 50 built-in data sets, and using predictive modeling techniques, the platform can collect and analyze data about learners and their contexts. This information is then used to provide decision-makers with data-driven insights to better their decisions and help optimize learning experiences.

DC 4: Disclosures about identified security incidents

There have been no known breaches identified as system incidents that (a) were the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements in last 12 months, as of August 18 2023.

DC 5: The applicable trust services criteria and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved

5.1 Integrity and Ethical Values

We uphold all to a high degree when it comes to Conduct and Ethics. Engaging in work practices that are fair and legal. Ensuring the best treatment of all employees by providing conditions which do not physically or mentally harm.

5.2 Commitment to Competence

We are committed to adding stellar employees to the team. This is done in a collaborative manner, looking beyond the resume, and focusing on relationships. Training and development are crucial to our continued success. We customize training by curating courses for specific roles. Evaluating an employee is the last step in our commitment to competence. Employee evaluations take place annually however, there are so many steps taken throughout the course of the year leading up to the evaluation such as collaboratively setting quarterly goals, manager & employee check-in's which are focused on getting you to reach your professional goals and receiving consistent feedback and mentorship from your manager. Ultimately, meeting throughout the year allows for successful evaluations.

5.3 Management's Philosophy and Operating Style (Culture of the company/ Leadership style/ website)

IntelliBoard Pro is comprised of data-loving, education-focused, and care-centric folks brilliant in the skills they bring to you. We dream BIG! We all share the same vision, but each provides a unique perspective. We strive to provide a well-rounded approach to all that we do.

5.4 Organizational Structure and Assignment of Authority and Responsibility (Job description and org chart/ HR policy)

Company operating model includes leadership composed of division leads and subordinate departments. Job descriptions and roles are decided on both standardized roles (sales, marketing, HR, development, QA, etc), as well as those defined internally based on need, e.g., Implementation Manager, Project Lead, Project Manager, etc. Our Job descriptions are specific and designed with the outlined requirements for the role along with what is needed to achieve the task. Allowing employees to gain perspective on the scope of work and how they will be measured.

5.5 Human Resource Policies and Practices

Employee performance reviews are given annually on an employee's anniversary date. It is crucial to an employee's success within their role to be given a review annually. During this review their manager will assess the employees' work habits, productivity, relationships with others, and if goals have been achieved.

5.6 Security Management

The Information Security Manager is a technical hands-on leader to all of our Information Security operations and processes. In this role, their responsibilities are to defend IntelliBoard Pro's platform and enterprise IT systems, including security intelligence, threat hunting, and advanced incident response functions. The Information Security Manager closely collaborates with many other teams within IntelliBoard Pro, as well as external customer security teams to actively defend IntelliBoard Pro's assets and the security of our customers.

5.7 Security and Privacy Policies

Information Security Policy (also known as "IT Security Policy")

intends to protect IntelliBoard Pro's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.Internet/Intranet/Extranet-related systems, including but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file transfers, are the property of IntelliBoard Pro, Inc. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.Effective security is a team effort involving the participation and support of every IntelliBoard Pro employee or contractor who deals with information and/or information systems. It is the responsibility of every team member to read and understand the policy, and to conduct their activities accordingly.

Privacy Policy

The IntelliBoard Pro platform imports personal data from its clients learning management systems, other client-permitted integrations and client uploaded data to the IntelliBoard Pro platform.
IntelliBoard Pro cares about your privacy. Privacy is a fundamental right for all individuals, globally. Our clients trust
us with the personal information of their employees, students, and other users within their respective systems.
We take the obligations that are attached to this information very seriously.
IntelliBoard Pro imports information from learning management systems, other client-permitted integrations and
client-uploaded data to the IntelliBoard Pro platform, for the explicit purpose of providing that information in a
format to be used exclusively by the client. We do not and will not sell or rent your data to third-parties unless
this is required in the context of changes to our business structure such as a merger or acquisition.
IntelliBoard Pro Privacy Principles

- IntelliBoard Pro does not sell client data.

- IntelliBoard Pro does not own the content you export to the IntelliBoard Pro platform. Clients are the only owners of their own data.
- IntelliBoard Pro consistently updates its security best practices to ensure ongoing protections.
- IntelliBoard Pro is compliant with FERPA, COPPA, CCPA and GDPR, among other privacy laws.
- IntelliBoard Pro is transparent about our practices.
- IntelliBoard Pro does not advertise within the IntelliBoard Pro platform.
- IntelliBoard Pro uses security practices that guide the certifications for both SOC II and ISO compliance.

5.8 Personnel Security

Background screenings are a part of our pre-boarding process, each employee is sent a "candidate link" which allows them to fill out their personal information for the criminal background check. During our onboarding process employees are signed up to receive all necessary trainings and given all policies which need to be reviewed and signed. All policies are reviewed, signed, and collected as a part of the onboarding process. Policies and training are then logged and stored in each employee's personnel file.

5.9 Physical Security and Environmental Controls

IntelliBoard Pro is primarily a remote company with no centralized headquarters or physical network. Because of this, physical and environmental security procedures have been deemed unnecessary. There are specific considerations taken, however, regarding remote work and the security risks inherent specific to companies that are fully remote. These can be found in our BYOD policy, our Business Continuity and Disaster Recovery plan, and our Information Security Policy.

5.10 Change Management

IntelliBoard Pro's Change Management policy aims to establish management direction and high-level objectives for the change management process. In addition, this policy guides the implementation of changes to reduce the impact on other tasks/projects as well as to mitigate associated risks such as:

- Information being corrupted and/or destroyed
- Adverse impact on other organizational processes
- Computer performance being disrupted and/or degraded
- Productivity losses being incurred

5.11 System Monitoring

IntelliBoard Pro utilizes AWS CloudWatch and AWS CloudTrail for system monitoring in the Amazon Web Services (AWS) cloud based solution. IntelliBoard Pro is also introducing the implementation of Hexnode Unified Endpoint Management (UEM) for all company owned devices or devices needing access to any part of IntelliBoard Pro's products, starting in 2024.

5.12 Incident Management

IntelliBoard Pro's Incident Management policy consists of a designated individual that establishes information security incident management within the organization, i.e., overseeing incident management activities, including documentation, response, escalation, resolution, and analysis.

IntelliBoard Pro will communicate where applicable with its employees, customers and other stakeholders when an incident that impacts them occurs, provide updates during the incident, and after the resolution.

As needed, the security incidents would be reported outside of IntelliBoard Pro by a designated person nominated by senior management.

Intrusion attempts, security breaches, theft or loss of hardware, suspicion of an incident or other security-related incidents perpetrated against the organization must be reported to our Incident Management team.
All known vulnerabilities, in addition to all suspected or known violations, must be communicated promptly.

Our Incident Management team responding to the incident shall perform incident handling activities consistent with the contingency plan of IntelliBoard Pro or IntelliBoard Pro's chain of custody procedure to ensure that the evidence gathered, both digital and physical, during the security or privacy incident can be used successfully during prosecution, if appropriate.

Whenever possible, IntelliBoard Pro shall use automated mechanisms to assist in collecting, tracking, analyzing and documenting all security incidents.

5.13 Data Backup and Recovery

Key objectives of the Business Continuity Plan (BCP) include the following:

1. Continuation of critical business operations in the event of an emergency.
2. Minimization of the duration of a serious disruption to operations and resources.
3. Minimization of damage and losses.
4. Facilitation of effective and efficient coordination of recovery tasks.
5. Ensuring effective recovery.

The goals of the Disaster Recovery Plan (DRP) are as follows:

A. To minimize interruptions to the normal operations.
B. To limit the extent of disruption and damage.
C. To minimize the economic impact of the interruption.
D. To establish alternative means of operation in advance.
E. To train personnel with emergency procedures.
F. To provide for smooth and rapid restoration of service.

Recovery Point Objective (RPO) & Recovery Time Objective (RTO) Level of Criticality – IntelliBoard Pro products are categorized into three levels of Criticality:
Tier-1: Mission-critical applications that require an RTPO of less than 4 hours
Tier-2: Business-critical applications that require RTO of 48 hours and RPO of 24 hours
Tier-3: Non-critical applications that require RTO of 120 hours and RPO of 24 hours

Name	Level of Criticality	Fixed Asset Y/N	Comments
IBPro	Tier 1	No	Application required for customers/businesses to function.

IBLite	Tier 1	No	Application required for customers/businesses to function.
IntelliCart	Tier 1	No	Application required for customers/businesses to function.
Client Portal	Tier 2	No	Functions can be managed manually within the IntelliBoard Pro product.

5.14 System Account Management

User access to information systems and IT assets shall be authorized based on their job roles and responsibilities and according to business requirements.
Access control to information systems and services shall cover all stages of the user access life-cycle: from granting and modifying user access to terminating access. Access to systems and IT assets shall be granted based on:

- Valid access authorization from the immediate supervisor or system owner.
- The concept of least privilege, allowing only authorized access for users (or processes acting on behalf of users), including privileged users, based on their job functions and intended system usage.
- Considering the separation of duties between individuals to prevent malicious activity without collusion and other attributes required by the organization or business function.
- Restricting user accounts from installing software on devices.
- Access to sensitive information such as personal information shall be restricted.
- Critical access such as privileged access, access to sensitive information shall be logged and access to these logs shall be restricted.
- Administration, system and generic accounts being strictly controlled and given based on authorization from designated personnel. IntelliBoard Pro shall authorize and monitor the use of guest/anonymous and temporary accounts.
- Temporary and inactive accounts that are no longer required and accounts of terminated or transferred users shall be deactivated promptly.

User Authentication and Secure Log-on Procedures

- Account access privileges (including service and generic accounts) shall be reviewed periodically.
- Access approval: IntelliBoard Pro shall follow a documented formal access approval process for granting or changing access privileges.
- Unnecessary services such as unused file sharing, web application modules or service functions must be disabled by the organization.
- Access to the IntelliBoard Pro information systems shall be controlled using password authentication or a public/private key system with a strong passphrase.
- Access control shall be centralized for all its assets through a directory service or single sign-on for organization asset.
- All users shall be assigned a unique user ID whenever possible and generic accounts should be avoided. The initial password provided by the administrator shall be changed at first login.
- Common device identifiers like Media Access Control (MAC), Internet Protocol (IP) addresses, or device-unique token identifiers, are used to uniquely identify individual, group, role, service, or device, based on authorization from a designated individual.

- Users shall not share their passwords with others or reveal the same to others under any circumstances. Passwords for user and administrator accounts shall be changed periodically, as applicable.
- Account lockout (temporary or unlimited) should be applied, whenever possible, after a defined number of unsuccessful login attempts.
- Users shall be automatically logged off from the information systems after a defined period of inactivity.
- At a minimum password shall be at least eight (8) characters long. For improved security, longer passwords should be used.
- Passwords shall contain alphanumeric and special characters (i.e., consider using passwords containing both upper- and lower-case characters (e.g., a-z, A-Z), have digits and punctuation characters as well as letters, e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Prohibit password reuse for a defined number of generations.
- Implement multi-factor authentication (MFA) for both privileged and non-privileged accounts, where possible.
- Appropriate IT personnel shall administer and manage administrator and system account passwords.
- User identity shall be verified before resetting any authentication credentials.
- Passwords for default system accounts shall be modified or disabled before installing a system on the network.
- Inventory of its authentication along with Multi Factor authentication (MFA) for third party applications and administrative accounts shall be enforced on all organization assets, reviewed and updated on an annual basis.
- Multi Factor authentication (MFA) shall be enforced for all administrative accounts, networks and third party applications

Termination

The organization shall consider creating a separation agreement to safeguard IntelliBoard Pro and its customers' Intellectual Property Rights and confidential information at the time of terminating their employment or business relationship with IntelliBoard Pro. The organization must, upon personnel termination, at least:

- Remove their access from any systems or applications that process sensitive information in a timely manner.
- Revoke all digital certificates.
- Ensure all tokens or smart cards issued are returned.
- Ensure that keys and IDs provided to them during their employment are returned.
- Remove all physical access to the facilities.
- Ensure that all devices, hardware and other material provided to them are returned.

5.15 Data Classification

Information in a final or published state that is either in the custody of or produced and owned by IntelliBoard Pro must be classified into one of the following three categories:

- Public: Information that is not confidential and can be made public without any implications for the organization. Such information is available to the public, employees, consultants and contractors without authorization.

- Internal: Information that is available to employees and authorized non-employees (consultants and contractors) possessing a need to know for business-related purposes.
- Confidential: Information that is sensitive (including personal information) within IntelliBoard Pro and is intended for use only by specified groups of employees. A breach of such information could cause serious embarrassment and possibly undermine public trust in the organization.

In some circumstances, confidential information may have to be disclosed to outsiders such as statutory auditors, external consultants, regulatory and legislative bodies, etc. The asset owner shall use their discretion to make the confidential information available and be responsible for getting such outsiders to sign Non-Disclosure Agreements (NDA). Even after such disclosure, the classification still remains 'confidential' and does not become 'public.'

5.16 Risk Management Responsibilities

System owners and department managers or supervisors are responsible for conducting a risk assessment as well as prioritizing, implementing and maintaining the appropriate risk-reduction measures defined in the risk assessment process.
Risk owners are the individuals who are ultimately accountable for ensuring the risk is managed appropriately. Multiple personnel may have direct responsibility for or oversight of, activities to manage each identified risk and collaborate with the accountable risk owner in their risk management efforts.
Executive Management is responsible for sponsoring and supporting the risk management plan and processes, participating in the risk management meetings, and reviewing and approving risk assessments and risk mitigation plans.
Responsibilities for the continued development, implementation and maintenance of the risk management program shall also be assigned internally.

5.17 Risk Management Program Activities

At a minimum, the risk management program shall focus on the following five types of activities:

- Identification of Strategic Objectives: The alignment of strategic objectives and risk management is essential to avoid a siloed risk management approach. This is the key step in performing risk assessments.
- Identification of Risks: A continuous effort to identify which risks are likely to affect IntelliBoard Pro's strategic objectives and consequently security functions and business continuity of IntelliBoard Pro and documenting their characteristics.
- Analysis of Risks: An estimation of the probability (likelihood), impact and prioritization of risks relative to each other. Review the risk management results periodically or whenever there are significant changes to the information system or other conditions that may impact the security state of the system.
- Mitigation Planning: Decisions and actions that will reduce the impact of risks and limit the probability of their occurrence or improve the response to a risk occurrence.
- Tracking and Controlling Risks: Collection and reporting of status information about risks and their mitigation plans, response to changes in risks over time, and management oversight of corrective measures taken in accordance with the mitigation plan.

5.18 Integration with Risk Assessment

IntelliBoard Pro shall establish a risk management framework aligned with business objectives that establish rules governing how to identify risks, assign risk ownership, how the risks impact the confidentiality, integrity and availability of the information and the method of treatment for identified risks. A formal risk assessment methodology shall be approved by management.
The risk management framework shall include guidelines for identifying and estimating the cost of protective measures to eliminate or reduce the security risks to an acceptable level.
All operations, products, services, information assets and information systems that are owned and operated by IntelliBoard Pro must be assessed for risks that result from threats to the integrity, availability and confidentiality of IntelliBoard Pro's data.

5.19 Information and Communications Systems

IntelliBoard Pro utilizes Microsoft Teams, Zoom, SharePoint, and OneDrive for communication and collaboration tools as well as to share files.

5.20 Data Communication

Encryption shall always be used to protect strictly confidential or sensitive information (such as personal information) transmitted over data networks to protect against risks of interception. This includes accessing network services requiring authentication (for example, usernames and passwords) or when otherwise sending or accessing strictly confidential information (for example, emails). IntelliBoard Pro shall implement defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal and state laws, directives, regulations, and standards.
Where confidential or sensitive data (such as personal information) is stored on or accessed from mobile devices (for example, laptops, tablets, smartphones, external hard drives, USB sticks, digital recorders), the devices themselves must be encrypted (using "full disk" encryption) irrespective of ownership.
Where strictly confidential data is stored in a public cloud-based storage facility, the data must be encrypted prior to storing to avoid unauthorized access. Where data is subject to an agreement with an external organization, the data should be handled (stored, transmitted or processed) following the organization's specific encryption requirements.
Encryption key lengths should use current industry-standard encryption algorithms for confidential or sensitive information.

5.21 Monitoring Controls

IntelliBoard Pro utilizes Amazon Inspector, AWS Security Hub, and Amazon GuardDuty, Snyk along with Pentest-Tools.com for weekly vulnerability assessments of all systems, applications, and networks within its AWS environment.

1. Amazon Inspector: The Information Security Team uses Amazon Inspector to automatically assess applications for vulnerabilities or deviations from best practices. After performing an assessment, a detailed report is produced and any critical issues are addressed as a priority.
2. AWS Security Hub: This service is used to provide a comprehensive view of the security state within AWS, allowing the team to check IntelliBoard Pro's environment against security industry

standards and best practices. It aggregates security findings from other AWS services like Amazon Inspector and Amazon GuardDuty.

3. Amazon GuardDuty: This threat detection service continuously monitors for malicious or unauthorized behavior. The Information Security Team uses GuardDuty to identify unexpected and potentially unauthorized or malicious activity within IntelliBoard Pro's AWS environment.
4. Pentest-Tools.com: Used to conduct additional vulnerability scans, providing a comprehensive scan of all systems for potential vulnerabilities. The results from pentest-tools.com are categorized and prioritized based on severity.
5. Snyk: The Information Security Team uses Snyk to identify and automatically fix vulnerabilities in IntelliBoard Pro's code, open source dependencies, and containers. Snyk is regularly run on the codebase as part of the continuous integration/continuous delivery (CI/CD) pipeline, ensuring that any new code contributions do not introduce new vulnerabilities.

Reports generated by Amazon Inspector, AWS Security Hub, Amazon GuardDuty, Snyk and Pentest-Tools.com are used to produce a comprehensive vulnerability assessment report. This report includes the list of vulnerabilities identified, their severity levels, and recommended mitigation measures. Remediations are implemented on a monthly basis with regards to how critical the vulnerability is that was found.

IntelliBoard Pro has also signed a contract with Prescient Security to obtain a completed penetration test report in 2024, before starting a SOC 2 Type 2 audit.

DC 6: Complementary User Entity Controls (CUECs):

IntelliBoard Pro's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to IntelliBoard Pro's services to be solely achieved by IntelliBoard Pro's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of IntelliBoard Pro.
The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

Trust Services Criteria	Complementary User Entity Controls
CC2.1	User entities are responsible for the security and integrity of data housed under user entity control, particularly the data utilized by IntelliBoard Pro systems and services.
CC6.2	Determination of personnel who need specific functionality and the granting of such functionality is the responsibility of authorized personnel at the user entity. This

	includes allowing access to IntelliBoard Pro's application keys and API keys for access to the web service API
CC6.3	Authorized users and their associated access are reviewed periodically
CC6.6	User entities will ensure protective measures are in place for their data as it traverses from user entity to IntelliBoard Pro.
CC6.6	User entities should establish adequate physical security and environmental controls of all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity in order to provide authorized information to IntelliBoard Pro.
C1.1	User entities assign responsibility to personnel, and those personnel identify which data used by IntelliBoard Pro is to be considered "sensitive".

DC 7: Complementary Subservice Organization Controls (CSOCs):

Although the subservice organization has been "carved out" for the purposes of this report, certain Trust Services Criteria are intended to be met by controls at the subservice organization. Complementary Subservice Organization Controls (CSOCs) are expected to be in place at AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities. Management of IntelliBoard Pro receives and reviews the AWS SOC 2 report annually. In addition, through its operational activities, IntelliBoard Pro management monitors the services performed by AWS to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to AWS/Google/Azure management.
It is not feasible for the criteria related to the System to be achieved solely by IntelliBoard Pro. Therefore, each user entity's internal control must be evaluated in conjunction with IntelliBoard Pro's controls and related tests, and results described in Section 4 of this report, considering the related CSOCs expected to be implemented at the subservice organization as described below.

Criteria	Complementary Subservice Organization Controls
CC6.4	AWS is responsible for restricting data center access to authorized personnel.
CC6.4	AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.

CC7.2 A1.2	AWS is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
CC7.2 A1.2	AWS is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
CC7.2 A1.2	AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

DC 8: Disclosures of out-of-scope Trust Services Criteria

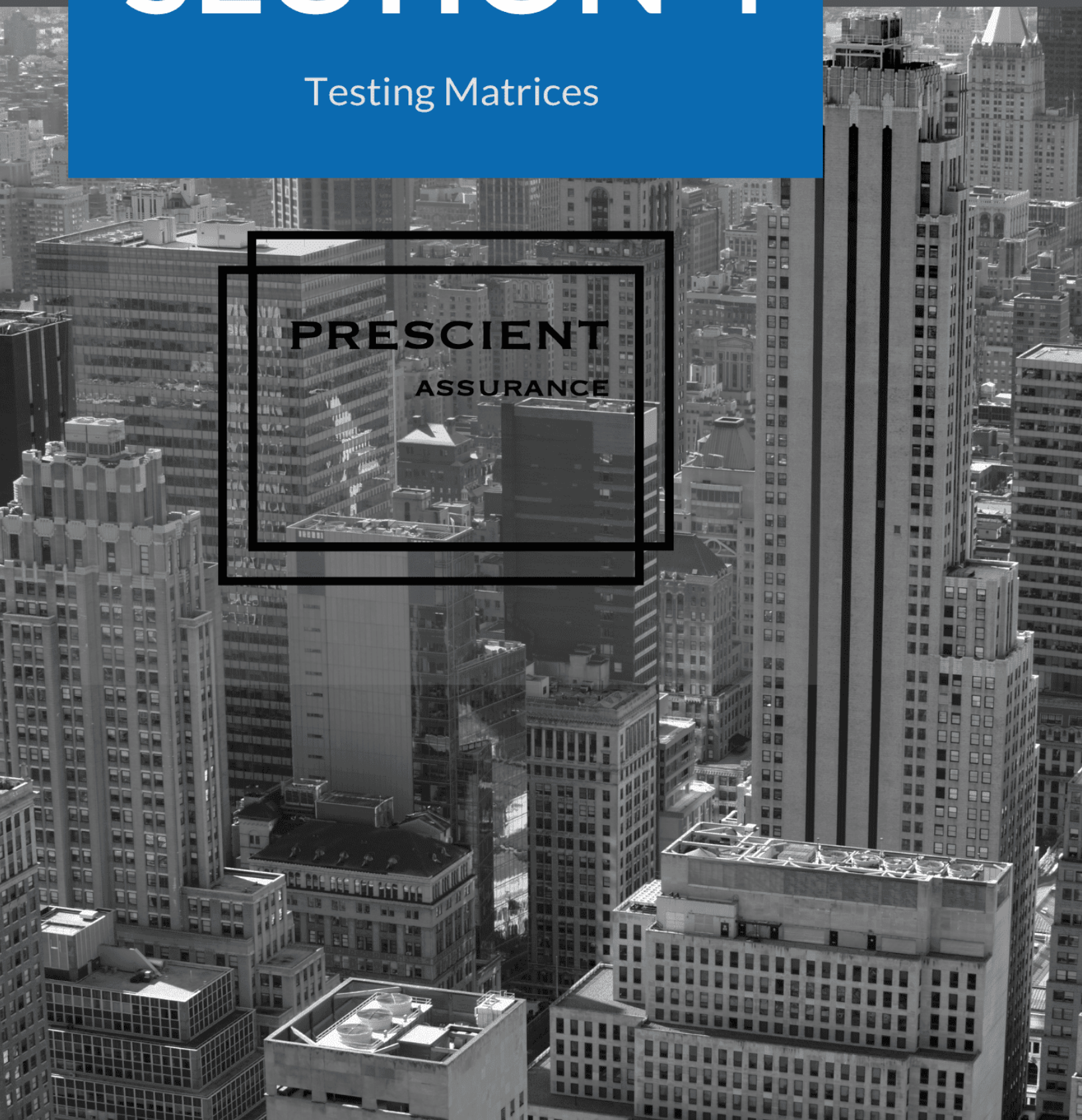
IntelliBoard Pro is primarily a remote company with no centralized headquarters or physical network. Because of this, physical and environmental security procedures have been deemed unnecessary. There are specific considerations taken, however, regarding remote work and the security risks inherent specific to companies that are fully remote. These can be found in our BYOD policy, our Business Continuity and Disaster Recovery plan, and our Information Security Policy.

DC 9: Disclosures of significant changes in last 1 year

IntelliBoard Pro has not had any significant changes in the last year that would affect our services that we provide.

SECTION 4

Testing Matrices



Tests of Design of Controls and Results of Tests

Scope of Testing

This report on the controls relates to IntelliBoard Pro Next provided by IntelliBoard Pro. The scope of the testing was restricted to IntelliBoard Pro Next, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing as of May 4, 2023.

The tests applied to test the design of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that all applicable trust services criteria were achieved during the review date. In selecting the tests of controls, Prescient Assurance LLC considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates.
- The control risk mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.
- The degree to which the control relies on the effectiveness of other controls.
- Whether the control is manually performed or automated.

Types of Tests Generally Performed

The table below describes the nature of our audit procedures and tests performed to evaluate the design of the controls detailed in the matrices that follow:

Test Types	Description of Tests
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: • Examination / Inspection of source documentation and authorizations to verify transactions processed. • Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures. • Examination / Inspection of systems documentation, configurations, and settings; and • Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.

Observation	Observed the implementation, application or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Re-performance	Re-performed the control to verify the design and / or operation of the control activity as performed if applicable.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices.

Any phrase other than this constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the Design of the control activity.

Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

Trust ID	COSO Principle	Control Description
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The organization has established communication channels that allow employees to securely and anonymously report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Third-party contractors working on behalf of the organization are required to sign an agreement outlining the standard code of conduct, security and confidentiality requirements.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The organization has established Acceptable Use and Corporate Ethics Policies which are both reviewed/updated on an annual basis by Executive Management. As part of the formal onboarding process, all employees are required to sign indicating their agreement and acknowledgment of the Acceptable Use and Corporate Ethics Policies and re-sign annually thereafter or in the event of any significant revisions.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The organization has defined a Code of Conduct and Ethics and reviews them annually.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The Board of Directors comprises of non-executive directors independent from management and meets on a quarterly basis for oversight on internal controls, operations and business objectives.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The Board of Directors' oversight responsibilities is defined and documented and acknowledged by the Board on an annual basis.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The executive team of the organization meets at planned intervals to discuss operations, issues relating to internal controls and delivery on key performance metrics.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Job descriptions that document the objectives of the role, responsibilities, reporting lines, employee qualifications and other requirements are made available to the employees. Job descriptions are reviewed and updated annually or in case of significant changes.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Information security roles and responsibilities of employees, contractors, and the organization are stated in contractual agreements.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Organization has established an organization chart that defines organizational roles, reporting lines, and authorities as it relates to development, quality assurance, and security operations of its services. The organization structure is reviewed and updated in case of significant changes.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The organization utilizes OneTrust platform to manage its Information Security policies and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The organization has a process in place to evaluate the competency of employees and identify their development needs regularly.

CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The organization has a formal training plan in place for the employees and meets annually to identify relevant training needs to support in scope-systems.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	New employees are subjected to background and reference checks prior to joining the organization.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A vendor management process has been implemented whereby management performs risk assessments of potential new vendors and evaluates the performance of existing vendors. Corrective actions are taken as required based on the results of the assessments.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Job descriptions that document the objectives of the role, responsibilities, reporting lines, employee qualifications and other requirements are made available to the employees. Job descriptions are reviewed and updated annually or in case of significant changes.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Employees are required to complete an information security and awareness training annually.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Information security roles and responsibilities of employees, contractors, and the organization are stated in contractual agreements.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The organization has a process in place to evaluate the competency of employees and identify their development needs regularly.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The organization has established communication channels that allow employees to securely and anonymously report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The organization uses OneTrust platform to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The organization has established Acceptable Use and Corporate Ethics Policies which are both reviewed/updated on an annual basis by Executive Management. As part of the formal onboarding process, all employees are required to sign indicating their agreement and acknowledgment of the Acceptable Use and Corporate Ethics Policies and re-sign annually thereafter or in the event of any significant revisions.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The organization has developed documentation and user guides that describe relevant system components as well as the purpose and design of the system. These documents are made available to both internal and external users and updated as needed.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Designated customer administrators and relevant organizational employees are trained on the functional use of the application

		to understand their roles and responsibilities as part of the onboarding process.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The organization uses OneTrust platform to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Information security roles and responsibilities of employees, contractors, and the organization are stated in contractual agreements.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The organization has developed documentation and user guides that describe relevant system components as well as the purpose and design of the system. These documents are made available to both internal and external users and updated as needed.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The organization has established communication channels that allow employees to securely and anonymously report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Employees are required to complete an information security and awareness training annually.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The organization has established Acceptable Use and Corporate Ethics Policies which are both reviewed/updated on an annual basis by Executive Management. As part of the formal onboarding process, all employees are required to sign indicating their agreement and acknowledgment of the Acceptable Use and Corporate Ethics Policies and re-sign annually thereafter or in the event of any significant revisions.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The Board of Directors comprises of non-executive directors independent from management and meets on a quarterly basis for oversight on internal controls, operations and business objectives.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The executive team of the organization meets at planned intervals to discuss operations, issues relating to internal controls and delivery on key performance metrics.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Changes that affect the functionality and security of the system components are communicated to internal and external users.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The organization utilizes OneTrust platform to manage its Information Security policies and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Third-party contractors working on behalf of the organization are required to sign an agreement outlining the standard code of conduct, security and confidentiality requirements.

CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated as required.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated as required.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The Board of Directors comprises of non-executive directors independent from management and meets on a quarterly basis for oversight on internal controls, operations and business objectives.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Designated customer administrators and relevant organizational employees are trained on the functional use of the application to understand their roles and responsibilities as part of the onboarding process.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The organization provides an external-facing support system that allows users to report incidents, complaints, issues, and any other challenge through an appropriate channel. Reported incidents are addressed by the organization's support staff in a timely manner.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The organization has developed documentation and user guides that describe relevant system components as well as the purpose and design of the system. These documents are made available to both internal and external users and updated as needed.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The organization has established communication channels that allow employees to securely and anonymously report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Information security roles and responsibilities of employees, contractors, and the organization are stated in contractual agreements.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	New customer contracts or modifications to existing customer contracts and end-user license agreements (EULA) are reviewed annually by Management to ensure security and confidentiality commitments are met.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The organization has formal agreements in place with customers which acknowledges their compliance on security, confidentiality and privacy commitments.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Management performs a formal risk assessment (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	A vendor management process has been implemented whereby management performs risk assessments of potential new vendors and evaluates the performance of existing vendors. Corrective actions are taken as required based on the results of the assessments.

CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Management performs a formal risk assessment (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Management performs a formal risk assessment (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Management performs a formal risk assessment (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	A vendor management process has been implemented whereby management performs risk assessments of potential new vendors and evaluates the performance of existing vendors. Corrective actions are taken as required based on the results of the assessments.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	A penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The executive team of the organization meets at planned intervals to discuss operations, issues relating to internal controls and delivery on key performance metrics.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The organization uses OneTrust platform to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Vulnerability scan is performed to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated in a timely manner.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The organization uses OneTrust platform to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.

CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The executive team of the organization meets at planned intervals to discuss operations, issues relating to internal controls and delivery on key performance metrics.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The organization uses OneTrust platform to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The organization uses OneTrust platform to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The organization uses OneTrust platform to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The executive team of the organization meets at planned intervals to discuss operations, issues relating to internal controls and delivery on key performance metrics.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The organization utilizes OneTrust platform to manage its Information Security policies and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Customer data is encrypted at rest (stored and backup) using strong encryption technologies.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The organization uses its cloud provider key management service to encrypt data at rest and to store and manage encryption keys. Access to production access keys is restricted to authorized individuals.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Encryption technologies are used to protect communication and transmission of data over public networks and between systems.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The organization maintains an inventory of production information assets including details on asset ownership, data classification and location. The asset inventory listing is reviewed and updated by management on an as-needed basis.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Unique user IDs and strong passwords are required in order to gain access to the infrastructure supporting the application (i.e. Active Directory, servers and database accounts).
CC6.1	The entity implements logical access security software, infrastructure, and architectures over	Management utilizes an employee termination checklist to ensure that the termination process is consistently executed,

	protected information assets to protect them from security events to meet the entity's objectives.	and access is revoked for terminated employees in a timely manner.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Disk encryption and system passwords are enabled across all organization workstations.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Access to in-scope system components (application(s) and its underlying infrastructure) requires a documented access request and approval from management prior to access provisioning.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Multi-factor authentication (MFA) is enforced for user accounts with administrative access to the organization's production platform.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	System components are configured such that the organization and its customers' access is appropriately segmented from other tenant users.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Unique user IDs and strong passwords are required in order to gain access to the application production environment.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	A formal network diagram outlining boundary protection mechanisms (e.g. firewalls, IDS, etc.) is maintained for all network connections and reviewed annually by IT management.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Management performs periodic user access review for in-scope system components to ensure that access is restricted appropriately. Access is modified or removed in a timely manner based on the results of the review.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Access to in-scope system components (application(s) and its underlying infrastructure) requires a documented access request and approval from management prior to access provisioning.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Management utilizes an employee termination checklist to ensure that the termination process is consistently executed, and access is revoked for terminated employees in a timely manner.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Access to promote changes to production is restricted to authorized personnel based on job responsibilities.

CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Management performs periodic user access review for in-scope system components to ensure that access is restricted appropriately. Access is modified or removed in a timely manner based on the results of the review.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Access to in-scope system components (application(s) and its underlying infrastructure) requires a documented access request and approval from management prior to access provisioning.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Access to a generic administrator or privileged accounts on the databases and servers supporting the application is restricted to authorized personnel based on a role-based access scheme.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Management utilizes an employee termination checklist to ensure that the termination process is consistently executed, and access is revoked for terminated employees in a timely manner.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Formal data retention and disposal policy and procedure are in place to guide the secure retention and disposal of information.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	A formal network diagram outlining boundary protection mechanisms (e.g. firewalls, IDS, etc.) is maintained for all network connections and reviewed annually by IT management.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The organization uses its cloud provider key management service to encrypt data at rest and to store and manage encryption keys. Access to production access keys is restricted to authorized individuals.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	System firewalls are configured on the application gateway and production network to limit unnecessary ports, protocols and services. Firewall rules are reviewed on an annual basis by IT management.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Intrusion detection or prevention systems are used to provide continuous monitoring of the company's network and to protect potential security breaches.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Encryption technologies are used to protect communication and transmission of data over public networks and between systems.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and	Encryption technologies are used to protect communication and transmission of data over public networks and between systems.

	external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Production data is not used in testing or development environments.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Customer data is encrypted at rest (stored and backup) using strong encryption technologies.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Disk encryption and system passwords are enabled across all organization workstations.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The organization uses its cloud provider key management service to encrypt data at rest and to store and manage encryption keys. Access to production access keys is restricted to authorized individuals.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Access to a generic administrator or privileged accounts on the databases and servers supporting the application is restricted to authorized personnel based on a role-based access scheme.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Antivirus software is in place to prevent or detect and act upon the introduction of unauthorized or malicious software.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Baseline configurations are retained within the configuration management tool for rollback capability anytime an approved configuration change is made.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Security software (firewall, anti-virus and anti-spam) is installed and enabled on all workstations.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	A formal change management process exists that governs changes to the applications and supporting infrastructure. The process document is reviewed by IT management on an annual basis and updated as needed.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	A log management process has been formalized to make sure that access to change the log configuration and access to modify logs is restricted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Baseline configurations are retained within the configuration management tool for rollback capability anytime an approved configuration change is made.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new	Vulnerability scan is performed to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated in a timely manner.

	vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	A penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Logging is enabled to monitor activities such as administrative activities, logon attempts, changes to functions, security configurations, permissions, and roles. Automated alerts are configured to notify IT management and issues identified are resolved in a timely manner through the incident management process.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	All incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with the formal incident management process
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Infrastructure has been configured to automatically scale the capacity and performance needs of the systems.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Intrusion detection or prevention systems are used to provide continuous monitoring of the company's network and to protect potential security breaches.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Logging is enabled to monitor activities such as administrative activities, logon attempts, changes to functions, security configurations, permissions, and roles. Automated alerts are configured to notify IT management and issues identified are resolved in a timely manner through the incident management process.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	System firewalls are configured on the application gateway and production network to limit unnecessary ports, protocols and services. Firewall rules are reviewed on an annual basis by IT management.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The IT team continuously monitors system capacity and performance through the use of monitoring tools to identify and detect anomalies that could compromise availability of the system operations. Incident management process is invoked for confirmed events and anomalies.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely

	objectives; anomalies are analyzed to determine whether they represent security events.	manner. The process document is reviewed by management on an annual basis and updated as required.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Notifications regarding confirmed data breaches are provided to affected data subjects, regulators, and other parties (as applicable) within an acceptable timeframe to meet the organization's privacy and confidentiality commitments.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	All incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with the formal incident management process
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Management incorporates lessons learned from ongoing incident response activities into incident response procedures on an ongoing basis.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated as required.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Vulnerability scan is performed to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated in a timely manner.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Management incorporates lessons learned from ongoing incident response activities into incident response procedures on an ongoing basis.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Notifications regarding confirmed data breaches are provided to affected data subjects, regulators, and other parties (as applicable) within an acceptable timeframe to meet the organization's privacy and confidentiality commitments.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Weekly full-system and daily incremental back-ups are performed using an automated system and replicated to an offsite location. Backups are monitored for failure using an automated system.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Disaster recovery plans (including restoration of backups) have been developed and tested regularly. Test results are reviewed and consequently contingency plans are updated.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The organization provides an external-facing support system that allows users to report incidents, complaints, issues, and any other challenge through an appropriate channel. Reported incidents are addressed by the organization's support staff in a timely manner.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated as required.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	All incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with the formal incident management process

CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Management has established defined roles and responsibilities to oversee the implementation of security policies including incident response.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	A patch management process exists to confirm that operating system level vulnerabilities are remediated in a timely manner. In addition, production servers are scanned to test patch compliance regularly.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	All incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with the formal incident management process
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	A patch management process exists to confirm that operating system level vulnerabilities for workstations are remediated in a timely manner. In addition, workstations are scanned to test patch compliance on a quarterly basis.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Management incorporates lessons learned from ongoing incident response activities into incident response procedures on an ongoing basis.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Access to promote changes to production is restricted to authorized personnel based on job responsibilities.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	A formal change management process exists that governs changes to the applications and supporting infrastructure. The process document is reviewed by IT management on an annual basis and updated as needed.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Emergency change requests are documented and subject to the standard change management process but at an accelerated timeline. Prior to initiating an emergency change, appropriate approval is obtained and documented.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	A formal system development life cycle (SDLC) methodology is established that governs the development, acquisition, implementation, and maintenance of application development and enhancement projects.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Changes that affect the functionality and security of the system components are communicated to internal and external users.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Changes to the application(s) and supporting infrastructure are documented, tested and approved by authorized personnel prior to implementation into the production environment in accordance with the change management process.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Changes to application and system infrastructure are developed and tested in a separate development or test environment before implementation.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Production data is not used in testing or development environments.

CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Baseline configurations are retained within the configuration management tool for rollback capability anytime an approved configuration change is made.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Management performs a formal risk assessment (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Management maintains insurance coverage through an external service provider against major financial risks for the overall business.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Vendor management process has been implemented that includes security procedures to be followed in case of vendor terminations.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	A vendor management process has been implemented whereby management performs risk assessments of potential new vendors and evaluates the performance of existing vendors. Corrective actions are taken as required based on the results of the assessments.