Service Organization Control Report - SOC2 Type 2

Report on ironSource Ltd.'s description of its Aura system and the suitability of the design of its controls relevant to Security, for the period December 01, 2023 to November 30, 2024

This report is intended solely for use by the management of ironSource Ltd. and the specified parties, and is not intended and should not be used by anyone other than these parties

Table of contents

Section I

Report of Independent Service Auditor

pwc

Report of Independent Service Auditors

To the Management of ironSource Ltd.

Scope

We have examined ironSource Ltd.'s (the "Service Organization") accompanying description of its Aura system (the "system") titled "ironSource Ltd.'s Description of Its Aura System" throughout the period December 01, 2023 to November 30, 2024 ("description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout that period, to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The Service Organization uses a subservice organization to provide cloud and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Service Organization, to achieve the Service Organization's service commitments and system requirements based on the applicable trust services criteria. The description presents the Service Organization's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Service Organization'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 or operating effectiveness of such complementary subservice organization controls.

Service organization's responsibilities

The Service Organization 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 the Service Organization's service commitments and system requirements were achieved. In Section II, the Service Organization has provided the accompanying assertion titled "Management of ironSource Ltd.'s Assertion" ("assertion"), about the description and the suitability of the design and operating effectiveness of controls stated therein. The Service Organization 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 and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. 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 and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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 and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements related to the 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 users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness 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.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section IV.

Opinion

In our opinion, in all material respects,

a. the description presents the system that was designed and implemented throughout the period December 01, 2023 to November 30, 2024, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period December 01, 2023 to November 30, 2024, to provide reasonable assurance that the Service Organization's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization applied the complementary controls assumed in the design of the Service Organization's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period December 01, 2023 to November 30, 2024, to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of the Service Organization's controls operated effectively throughout that period.

Restricted use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of ironSource Ltd., user entities of the system during some or all of the period December 01, 2023 to November 30, 2024, business partners of ironSource Ltd. 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 ("specified parties"), if applicable:

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

This report is not intended to be, and should not be, used by anyone other than these specified parties. If a report recipient is not a specified party as defined above and has obtained this report, or has access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Kesselman & Kesselman, Certified Public Accountants (Isr.) as a result of such access. Further, Kesselman & Kesselman, Certified Public Accountants (Isr.) does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Tel-Aviv, Israel
March 05, 2025

Kesselman & Kesselman
Certified Public Accountants (lsr.)
A member firm of PricewaterhouseCoopers International Limited

Section II

Management's Assertion

Management of ironSource Ltd.'s Assertion

We have prepared the accompanying description of ironSource Ltd.'s Aura system (the "system") titled "ironSource Ltd.'s Description of Its Aura System" throughout the period December 01, 2023 to November 30, 2024, ("description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"). The description is intended to provide user entities with information about the system that may be useful when assessing the risks arising from interactions with the system, particularly information about system controls that ironSource Ltd. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* (AICPA, *Trust Services Criteria*).

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

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

a. the description presents the system that was designed and implemented throughout the period December 01, 2023 to November 30, 2024, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period December 01, 2023 to November 30, 2024, to provide reasonable assurance that ironSource Ltd.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization applied the complementary controls assumed in the design of ironSource Ltd.'s controls throughout that period.

c. the controls stated in the description operated effectively throughout the period December 01, 2023 to November 30, 2024, to provide reasonable assurance that ironSource Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of ironSource Ltd.'s controls operated effectively throughout that period.

Signed by:
Moni Givol
588F142D4E114E4...

Moni Givol, CISO

Section III

Service Organization's Description of its System

Type of Services Provided

The Aura system ("Aura") from Unity Technologies SF ("Unity" or "the Company") provides a platform for Android manufacturers (Original Equipment Manufacturers [OEMs]) and cellular network operators (carriers) that enables them to engage with their customers throughout the device lifetime. Carriers and OEMs (publishers or supply) use Aura to promote key services outside the store, directly on-device, by suggesting content from Android application developers (advertisers or demand) to the users on the initial device setup using Aura's Out Of the Box Experience (OOBE) and throughout the device lifetime by showing engaging notifications and other on-device applications and experiences like Aura News. OOBE, and Aura News each have their own on-device Android client application and supporting backend.

OOBE
Aura OOBE is an Android application that is part of the device setup and that works as a recommendation platform for applications according to the user's age, gender, device type, and location. Aura uses these parameters on the backend to tailor its application recommendations for the users and help them set up their device with relevant applications, including top rated and popular applications, as well as the OEM/carrier's branded applications.

Aura News
Aura News is a content discovery application covering content from breaking news headlines to lifestyle and magazine content creating a personalized content feed based on the user's interests and activity. The content is curated from multiple external news providers using an application programming interface (API).

Supporting Systems

Content Management System
The Content Management System (CMS) is an internal system that provides full control over the content and functionality of Aura. The CMS enables the management of applications, control over configuration parameters, the look and feel of the experience, and overall management of the different settings of engagement with the user.

Campaign Management
The Campaign Management (CM) system is an internal system used to add/edit advertisers and their budgets and settings (contact name, address, etc.) and to add/edit campaigns for each advertiser.
The main capabilities of the CM are:

- Targeting settings (e.g., countries of reach, device models, age, gender, etc.)
- Budget settings (e.g., the daily, weekly, monthly, and overall campaign spend)
- Campaign settings (start/end dates, creative assets, texts, etc.)

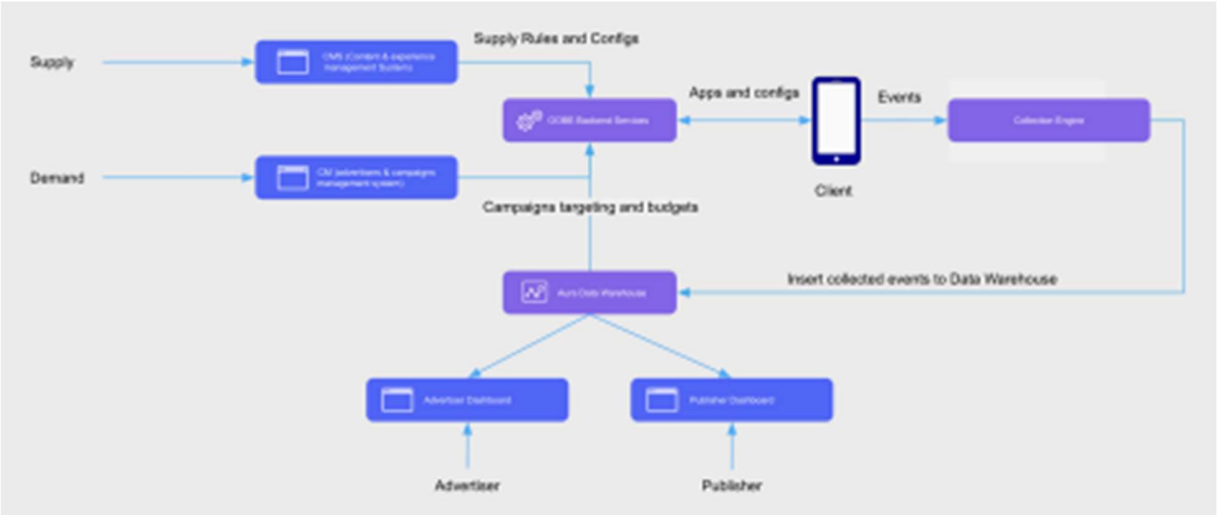
Advertisers Dashboard
The Advertisers Dashboard is an external-facing dashboard for Aura's advertisers providing views of daily analytics and trends, campaign management and performance insights, and a view into the advertiser's spends with Aura. The dashboard's backend receives the data used for the analytics from an internal backend reporting service. The dashboard's login mechanism is based on Amazon Web Services (AWS) Cognito service.

Publishers Dashboard
The Publisher Dashboard is an external-facing dashboard for Aura's publishers providing views of daily analytics and trends, product engagement metrics, and a view into the publisher's revenues with Aura. The dashboard's backend receives the data used for the analytics from an internal backend reporting service. The publisher dashboard's login mechanism is based on AWS Cognito service.

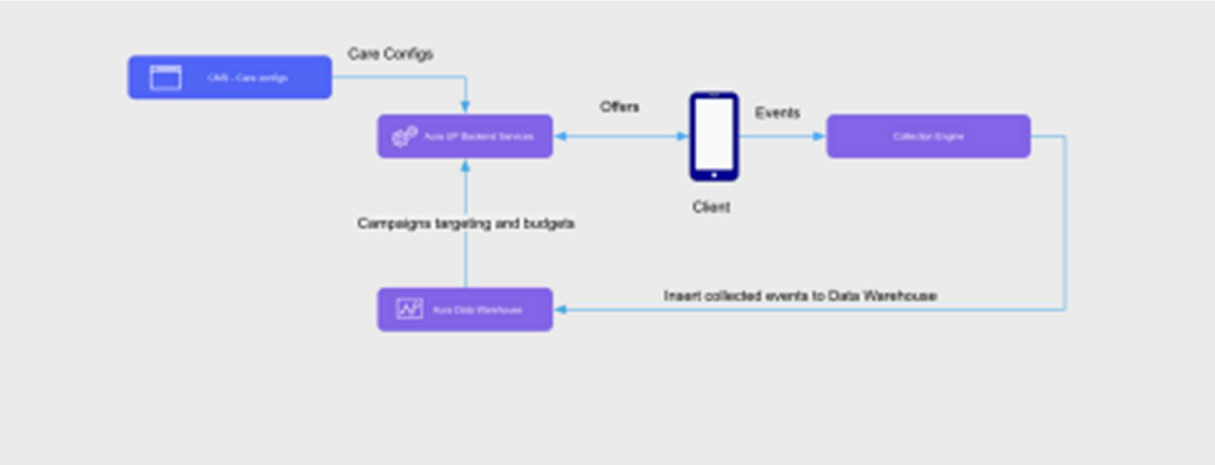
The Aura client applications (OOBE, AuraNews) send data about the user interaction through Aura's Data Collection Engine (ACE). This system is a data pipeline, receiving events sent from Aura's client applications and sending them to Aura's databases, providing a highly available and resilient data collection and management service. The integration of the client application to ACE is made via HTTPS rest API calls that are made every time the client collects enough data, or a specific timeframe has passed since the last recorded user interaction. Every event that was recorded via ACE will eventually be inserted to Aura's data warehouse and will be used to analyze and further optimize the user experience.

The following diagrams depict the high level structure of Aura OOBE, and Aura News.

Aura OOBE



Aura News



The system description in this section of the report details the Aura system. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organization.

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Aura system. Commitments are communicated in the Company's Software License Agreement and Data Protection Addendums.

System requirements are specifications regarding how the Aura system should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the Aura system include the following:

Trust Services Category	Service Commitments	System Requirements
Security	The Company will implement appropriate technical, organizational, and administrative controls and safeguards designed to ensure the security of customer data by protecting against unauthorized loss, misuse, disclosure, alteration, unauthorized access, and destruction.	Logical access standards Physical access standards Employee provisioning and deprovisioning standards Access review standards Encryption standards Intrusion detection standards Risk and vulnerability management standards Configuration management standards Incident handling standards Change management standards Vendor management standards

The Components of the System Used to Provide the Services.
The boundaries of the Aura system are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Aura System.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure
The Aura system is deployed on Amazon Elastic Compute Cloud (EC2) instances in Aura's AWS Cloud account. The Aura system uses AWS' hosted database and cache servers and industry standard tools. Employees' access is based on AWS Identity and Access Management (IAM) on a need-to-know basis. Data is encrypted according to the data classification policy both at rest and in transit, using industry standards by using AWS encryption tools and secured protocols.

Software

Software consists of the programs and software that support Aura (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor Aura include the following applications, as shown in the table below:

Software	
Splunk On-Call	Application and Infrastructure monitoring
Sumo Logic	Security information and event management (SIEM)
CrowdStrike (user endpoints)	Anti-malware
Amazon GuardDuty	Intrusion detection
Orca	Vulnerability Management, Cloud Compliance and Posture Management, Cloud Workload Protection
Jira	Help desk and ticketing system
Jenkins, Rundeck	Build pipeline
GitHub	Code repository
Pulumi	Infrastructure as a code
Okta, Duo	Identity Management (single sign-on [SSO]), multi-factor authentication (MFA)
Global Protect	Virtual private network (VPN)

People

Unity has two main divisions, Create and Grow. Create focuses on helping creators to create real-time three-dimensional (3D) content, and Grow helps customers and creators to grow their business.

Aura is a division focused on the OEMs and carriers market. Each division is an independent profit and loss entity, but all divisions have cross-company services such as Information Technology (IT) and Human Resources (HR) organized in the following functional areas:

Research and Development:

- Development – The software development staff develops and maintains the custom software for Aura. This includes the Aura user interface developers and core services developers who are responsible for the integration of Aura in Android phones.

- Product – The product staff plans the Aura future roadmap, monitors day to day development, and plans the releases and deployments timeline.

Operations:

- Sales – The sales team manages sales strategy and goals for the Aura division. ● Performance - The performance team manages the content of the Aura system across customers.

General and Administration (Cross-Company Services):

- HR – HR monitors the Company code of conduct; recruits employees; manages employee's engagement, compensation, and benefits; and maintains the Company's culture.
- IT – IT supports the computers and servers and performs IT support for the Company.

Subservice Organization and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS as a subservice organization for data center colocation services. The Company's controls related to the Aura system cover only a portion of the overall internal control for each user entity of the Aura system. The description does not extend to the colocation services for IT infrastructure provided by the subservice organization.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at AWS related to physical security and environmental protection. AWS' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the AWS SOC 2 report annually. In addition, through its operational activities, Company management monitors the services performed by AWS to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS management. It is not feasible for the service commitments, system requirements, and applicable criteria related to the Aura system to be achieved solely by the Company. The CSOCs that are expected to be implemented at AWS are described below.

Criteria	**Complementary Subservice Organization Controls**
CC6.1	AWS encrypts databases in its control.
CC6.4	● AWS restricts data center access to authorized personnel. ● AWS monitors data centers 24/7 by closed circuit cameras and security personnel.
CC6.5 CC6.7	AWS securely decommissions and physically destroys production assets in its control.

Criteria	Complementary Subservice Organization Controls
CC7.2	● AWS installs fire suppression and detection and environmental monitoring systems at its data centers. ● AWS protects data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). ● AWS oversees the regular maintenance of environmental protections at its data centers.

Section IV

Trust Services Category, Criteria and Related Controls

Applicable Trust Services Criteria Relevant to Security

The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

Security refers to the protection of:

- *information* during its collection or creation, use, processing, transmission, and storage, and
- *systems* that use electronic information to process, transmit or transfer, and store information to enable the achievement of ironSource Ltd.'s service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
	CONTROL ENVIRONMENT			
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	IS0069	Unity has implemented a Code of Conduct and Ethics document that describes responsibilities and expected behavior regarding data and information system usage.	Inspected the employee handbook and confirmed it includes the Code of Conduct and Ethical policy. Confirmed the handbook details the terms and conditions of employment, and the Code details the employee's expected behavior. No exceptions noted.
		IS0096	A formalized whistleblower policy is established, and an anonymous communication channel is available for employees to report potential security issues or fraud concerns.	Inspected the Code of Conduct and Ethical policy. Confirmed an anonymous communication channel is mentioned in the Code. Confirmed the code was reviewed throughout the audited period. No exceptions noted.
		IS0101	As part of the onboarding process, new employees sign on confidentiality requirements.	Observed the employee's NDA template to confirm each employee is required to sign and acknowledge the confidentiality requirements as part of their hiring process. No Exceptions noted.
		IS0111	As part of the onboarding process, the Company communicates a handbook with significant policies to the new employees.	Obtained a list of the company's employees, sampled new employees who joined throughout the audited period, and confirmed the sampled employees read and acknowledged the Code of Conduct, non-disclosure agreement, and the employee's handbook. No Exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0090	The Company has documented disciplinary actions in a formalized sanctions policy for employees and contractors who violate the code of conduct.	Inspected the Code of Conduct and confirmed that the Code includes description of potential sanctions and a designated function who is responsible to monitor compliance with the Code, including contact details and reporting channels. No exceptions noted.
		IS0071	Formal policies and procedures that outline the requirements for vendor management are documented and include the following components: Maintaining a list of critical vendors, Requirements for critical vendors to maintain their own security practices and procedures, annually reviewing attestation reports for critical vendors or performing a vendor risk assessment.	Inspected a database detailing the vendor risk assessment work performed by the Company to confirm that it includes identified risks, owners and mitigation plans. No exceptions noted.
		IS0124	Periodically, Management assesses critical third-party vendors to confirm they comply with security commitments and requirements.	Inspected a database detailing the vendor risk assessment work performed by the Company to confirm that it includes identified risks, owners and mitigation plans. No exceptions noted.
		IS1282	Before contracting with a new vendor, Management verifies that the agreement with the new vendor includes a NDA and confidentiality requirements, as well as an acknowledgement of the Code of Conduct.	Sampled critical vendors to confirm that the sampled vendors signed on a non-disclosure agreement (NDA). No exceptions noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	IS0098	The board of directors meets quarterly and maintains formal meeting minutes. The board includes directors that are independent of the Company.	Observed sampled Board meetings presentations, and confirmed that the Board discussed items related to risks, controls, changes and mitigation activities where relevant. Confirmed that for the sampled Board meetings, meeting minutes were documented and shared with the Board members. Confirmed that some Board members are independent from Management. No exceptions noted.
		IS0646	The Board of Directors include independent members, according to the Board of Directors' Charter, in order to maintain independence from management.	Inspected the list of directors to confirm that there are independent Board members in the Board of Directors. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0113	The board of directors understands and acknowledges its oversight responsibilities in relation to established requirements and expectations, as described in the board of directors' charter.	Inspected the AOA document to confirm that it states the Board's oversight responsibilities, and to confirm the Board members reviewed and approved the document. No exceptions noted.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	IS0068	The Company's Organization Structure and Reporting lines are updated regularly. The Organization Structure and Reporting lines' information is available for employees through HR systems.	Inspected the company's Organizational Chart and confirmed it details the roles and the reporting channels of the company. Confirmed that the Organizational Chart was approved by Management throughout the audited period. No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	IS0022	Unity's policy and procedure manuals address controls over significant aspects of operations. Policy sections include: Risk Management policy, Access and Authorization policy, Data Classification policy, Change Management policy, Code Of Conduct and Ethics document, Roles and Responsibilities document, Incident Response procedures.	Obtained relevant policies and confirmed they were properly reviewed and approved by management and are available for the company's employees. No exceptions noted.
		IS0165	The company uses a central repository to retain policies and procedures. The repository is accessible to relevant employees.	Observed the Confluence tool to confirm all relevant policies are managed through the tool and available to relevant employees. No exceptions noted.
		IS0108	Job requirements are documented in the job descriptions. Each candidate's job requirements are evaluated as part of the hiring process to support the achievement of objectives.	Inspected the job descriptions of several candidates and confirmed they were evaluated as part of the hiring process. No exceptions noted
		IS0110	New employees and contractors offered employment are subject to background checks prior to their start date.	Sampled new employees who joined the company throughout the audited period and inspected evidence of the recruitment process to confirm background checks were performed where applicable. No exceptions noted.
		IS0109	At least annually, a review process is in place for the Company's employees. As part of this process, Management reviews the employees' performance and skills.	Obtained an HR list of employees and confirmed that for sampled employees a performance assessment was performed throughout the audited period. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0100	The Company provides security awareness training for new hires upon hire and annually for current employees to support the achievement of objectives.	Obtained the security training invitation, list of participants and security training presentation to confirm a training was performed throughout the audited period. No exceptions noted.
		IS0113	The board of directors understands and acknowledges its oversight responsibilities in relation to established requirements and expectations, as described in the board of directors' charter.	Inspected the AOA document to confirm that it states the Board's oversight responsibilities, and to confirm the Board members reviewed and approved the document. No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	IS0068	The Company's Organization Structure and Reporting lines are updated regularly. The Organization Structure and Reporting lines' information is available for employees through HR systems.	Inspected the company's Organizational Chart and confirmed it details the roles and the reporting channels of the company. Confirmed that the Organizational Chart was approved by Management throughout the audited period. No exceptions noted.
		IS0109	At least annually, a review process is in place for the Company's employees. As part of this process, Management reviews the employees' performance and skills.	Obtained an HR list of employees and confirmed that for sampled employees a performance assessment was performed throughout the audited period. No exceptions noted.
	COMMUNICATION AND INFORMATION			
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	IS0072	The company performs a self-assessment to confirm the controls meet the organization's policies and operate effectively.	Observed controls matrices, lists of relevant procedures related to these controls, and internal test results, to confirm that the company assesses information required to support SOC 2 controls. No exceptions noted.
		IS0793	Infrastructure and application monitoring tools are utilized to monitor system, infrastructure, and application availability and performance and generates alerts when specific, predefined thresholds are met.	Observed the system's monitoring dashboard and confirmed it contains real time status of relevant system components, including disk space, utilization, performance, and other metrics. No exceptions noted.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	IS0022	Unity's policy and procedure manuals address controls over significant aspects of operations. Policy sections include: Risk Management policy, Access and Authorization policy, Data Classification policy, Change Management policy, Code Of Conduct and Ethics document, Roles and Responsibilities document, Incident Response procedures.	Obtained relevant policies and confirmed they were properly reviewed and approved by management and are available for the company's employees. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0165	The company uses a central repository to retain policies and procedures. The repository is accessible to relevant employees.	Observed the Confluence tool to confirm all relevant policies are managed through the tool and available to relevant employees. No exceptions noted.
		IS0098	The board of directors meets quarterly and maintains formal meeting minutes. The board includes directors that are independent of the Company.	Observed sampled Board meetings presentations and confirmed that the Board discussed items related to risks, controls, changes and mitigation activities where relevant. Confirmed that for the sampled Board meetings, meeting minutes were documented and shared with the Board members. Confirmed that some Board members are independent from Management. No exceptions noted.
		IS0068	The Company's Organization Structure and Reporting lines are updated regularly. The Organization Structure and Reporting lines' information is available for employees through HR systems.	Inspected the company's Organizational Chart and confirmed it details the roles and the reporting channels of the company. Confirmed that the Organizational Chart was approved by Management throughout the audited period. No exceptions noted.
		IS0100	The Company provides security awareness training for new hires upon hire and annually for current employees to support the achievement of objectives.	Obtained the security training invitation, list of participants and security training presentation to confirm a training was performed throughout the audited period. No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	IS0092	The user interface includes an option to contact customer support or management, providing them relevant information	Inspected the system's user interface and confirmed it includes an option to contact the company. No exceptions noted.
		IS0121	The company provides guidelines and technical support resources related to system operations to its customers and users.	Obtained publicly available guidelines and technical support resources related to system operations and confirmed the documents include a product overview, objectives and features, how-to guides, and FAQs. No exceptions noted.
		IS1443	As needed, the Company updates the customers about critical changes, down time, systems failures, and incidents.	Inspected the company's knowledge base for customers and confirmed that the customers can get updates and relevant information regarding the platform, changes to the platform, information about incidents or down time and more through this knowledge base. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
	RISK ASSESSMENT			
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	IS0020	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected a database detailing the risk assessment work performed by the Company to confirm that it includes identified risks, owners and mitigation plans. Inquired about the identified risks to confirm they deem relevant to the system activity and environment. No exceptions noted.
		IS0068	The Company's Organization Structure and Reporting lines are updated regularly. The Organization Structure and Reporting lines' information is available for employees through HR systems.	Inspected the company's Organizational Chart and confirmed it details the roles and the reporting channels of the company. Confirmed that the Organizational Chart was approved by Management throughout the audited period. No exceptions noted.
		IS0098	The board of directors meets quarterly and maintains formal meeting minutes. The board includes directors that are independent of the Company.	Observed sampled Board meetings presentations and confirmed that the Board discussed items related to risks, controls, changes and mitigation activities where relevant. Confirmed that for the sampled Board meetings, meeting minutes were documented and shared with the Board members. Confirmed that some Board members are independent from Management. No exceptions noted.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	IS0020	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected a database detailing the risk assessment work performed by the Company to confirm that it includes identified risks, owners and mitigation plans. Inquired about the identified risks to confirm they deem relevant to the system activity and environment. No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	IS0020	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected a database detailing the risk assessment work performed by the Company to confirm that it includes identified risks, owners and mitigation plans. Inquired about the identified risks to confirm they deem relevant to the system activity and environment. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0097	Annually, access rights to in-scope systems are reviewed and approved. In case of exceptions identified, actions are taken to resolve the issue.	Inspected evidence of the core systems review and confirmed that the CTO reviewed and approved the users and their access permissions during the audit period. No exceptions noted.
		IS0007	Annually, privileged access to the system is reviewed and approved by Management.	Inspected a list of users with privileged access to the network and infrastructure and confirmed this list was reviewed and approved by Management throughout the audited period. No exceptions noted.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	IS0020	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected a database detailing the risk assessment work performed by the Company to confirm that it includes identified risks, owners and mitigation plans. Inquired about the identified risks to confirm they deem relevant to the system activity and environment. No exceptions noted.
	MONITORING ACTIVITIES			
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	IS0072	The company performs a self-assessment to confirm the controls meet the organization's policies and operate effectively.	Observed controls matrices, lists of relevant procedures related to these controls, and internal test results, to confirm that the company assesses information required to support SOC 2 controls. No exceptions noted.
		IS0015	Formal procedures that outline requirements for vulnerability management are documented and include the following components: Methods for identifying vulnerabilities and frequency, Assessing the severity of identified vulnerabilities, Prioritizing and implementing remediation or mitigation activities for identified vulnerabilities based on severity and defined timelines.	Inspected the latest internal penetration test report to confirm that an internal penetration test was performed during the past year. confirmed that high / critical observations were properly addressed in a timely manner. No exceptions noted.
		IS0545	At least annually, an external penetration test is performed by the security team. The results of the external penetration test, including the risks identified and action items, are communicated to management. High and critical deficiencies are handled via Jira tickets.	Inspected the latest external penetration test report to confirm that an external penetration test was performed during the past year. Confirmed that there were no moderate/high/critical observations in the report results. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0009	The company has implemented a designated tool in order to identify new vulnerabilities before moving the change into the staging environments.	Inspected the tool used for code vulnerability scans and its settings to confirm the tool is in place and is set to review vulnerabilities in codes prior to deployment to production. No exceptions noted.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	IS0098	The board of directors meets quarterly and maintains formal meeting minutes. The board includes directors that are independent of the Company.	Observed sampled Board meetings presentations, and confirmed that the Board discussed items related to risks, controls, changes and mitigation activities where relevant. Confirmed that for the sampled Board meetings, meeting minutes were documented and shared with the Board members. Confirmed that some Board members are independent from Management. No exceptions noted.
		IS0015	Formal procedures that outline requirements for vulnerability management are documented and include the following components: Methods for identifying vulnerabilities and frequency, Assessing the severity of identified vulnerabilities, Prioritizing and implementing remediation or mitigation activities for identified vulnerabilities based on severity and defined timelines.	Inspected the latest internal penetration test report to confirm that an internal penetration test was performed during the past year. confirmed that high / critical observations were properly addressed in a timely manner. No exceptions noted.
		IS0545	At least annually, an external penetration test is performed by the security team. The results of the external penetration test, including the risks identified and action items, are communicated to management. High and critical deficiencies are handled via Jira tickets.	Inspected the latest external penetration test report to confirm that an external penetration test was performed during the past year. Confirmed that there were no moderate/high/critical observations in the report results. No exceptions noted.
	CONTROL ACTIVITIES			
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	IS0020	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected a database detailing the risk assessment work performed by the Company to confirm that it includes identified risks, owners and mitigation plans. Inquired about the identified risks to confirm they deem relevant to the system activity and environment. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0072	The company performs a self-assessment to confirm the controls meet the organization's policies and operate effectively.	Observed controls matrices, lists of relevant procedures related to these controls, and internal test results, to confirm that the company assesses information required to support SOC 2 controls. No exceptions noted.
		IS0097	Annually, access rights to in-scope systems are reviewed and approved. In case of exceptions identified, actions are taken to resolve the issue.	Inspected evidence of the core systems review and confirmed that the CTO reviewed and approved the users and their access permissions during the audit period. No exceptions noted.
		IS0007	Annually, privileged access to the system is reviewed and approved by Management.	Inspected a list of users with privileged access to the network and infrastructure and confirmed this list was reviewed and approved by Management throughout the audited period. No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	IS0020	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected a database detailing the risk assessment work performed by the Company to confirm that it includes identified risks, owners and mitigation plans. Inquired about the identified risks to confirm they deem relevant to the system activity and environment. No exceptions noted.
		IS0048	The Company utilizes a designated monitoring tool in order to enable activities investigation. The activities log is retained for 90 days.	Observed AWS CloudTrail system used by the company to confirm that the company monitors security and operation actions and user activity in the system. Observed log settings and confirmed the logs are retained for 90 days. No exceptions noted.
		IS0602	A SIEM tool is in place to alert when a sensitive activity or a security threat is identified.	Observed SUMO Logic configuration to confirm alerts are in place for critical activities such as login failures, capacity issues etc. No exceptions noted.
		IS0605	The Company utilizes a designated monitoring tool in order to enable activities investigation. The activities log is retained for 90 days.	Observed SUMO logic tool used by the company to confirm that the company monitors security and operation actions and user activity in the system. Observed log settings and confirmed the logs are retained for 90 days. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0607	The monitoring tool provides a dashboard representing a timely, accurate and current data processed in the system.	Observed the SUMO logic tool's monitoring dashboard and confirmed it contains real time status of all the system components. No exceptions noted.
		IS0621	Access to the SIEM monitoring tool is restricted only to authorized personnel.	Observed SUMO Logic tool's login configuration and confirmed access to alter or change the tool is limited to appropriate personnel, and is password protected. No exceptions noted.
		IS0002	The Company implements a baseline configuration for servers in order to define a standard level of service and security configuration for each server.	Inspected the configuration management tool to confirm that the company uses a baseline configuration in order to define a standard level of service and security configurations over the servers. No exceptions noted.
		IS0077	The Company maintains a server configuration and hardening policy for system components in-scope, with relevant configuration required to meet the company's objectives.	Inspected the Server Security Standard document and confirmed that it includes guidelines required for endpoints in the areas of security parameters, removal of unnecessary ports etc. No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	IS0022	Unity's policy and procedure manuals address controls over significant aspects of operations. Policy sections include: Risk Management policy, Access and Authorization policy, Data Classification policy, Change Management policy, Code Of Conduct and Ethics document, Roles and Responsibilities document, Incident Response procedures.	Obtained relevant policies and confirmed they were properly reviewed and approved by management and are available for the company's employees. No exceptions noted.
		IS0068	The Company's Organization Structure and Reporting lines are updated regularly. The Organization Structure and Reporting lines' information is available for employees through HR systems.	Inspected the company's Organizational Chart and confirmed it details the roles and the reporting channels of the company. Confirmed that the Organizational Chart was approved by Management throughout the audited period. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0098	The board of directors meets quarterly and maintains formal meeting minutes. The board includes directors that are independent of the Company.	Observed sampled Board meetings presentations and confirmed that the Board discussed items related to risks, controls, changes and mitigation activities where relevant. Confirmed that for the sampled Board meetings, meeting minutes were documented and shared with the Board members. Confirmed that some Board members are independent from Management. No exceptions noted.
	Logical and Physical Access Controls			
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	IS0473	In-scope system components require unique username and passwords (or authorized SSH keys) prior to authenticating users.	Inspected the mechanism used for user identification (in Okta) and confirmed that in-scope system users, including operating systems and databases, are identified through a user ID and a password. No exceptions noted.
		IS0675	The company maintains a list of digital assets that includes the asset owner, sensitive information etc. Annually, VP R&D reviews and approves the list of digital assets as part of the risk assessment process to identify key information system processes. New digital assets are assessed and approved prior to implementation. Digital assets which are not in use are removed and access to these assets is disabled.	Inspected the digital assets list to confirm the company maintains a master list of the entity's assets and services. No exceptions noted.
		IS0764	The company implements an Access and Authorization policy. The policy is reviewed and approved by the relevant personnel annually. In addition, the policy is available for the relevant employees.	Inspected the company's Security Policy and confirmed that the security policy details procedures around access management. Confirmed that the policy was reviewed and approved by Management. No exceptions noted.
		IS0473	In-scope system components require unique username and passwords (or authorized SSH keys) prior to authenticating users.	Inspected the mechanism used for user identification (in Okta) and confirmed that in-scope system users, including operating systems and databases, are identified through a user ID and a password. No exceptions noted.
		IS0097	Annually, access rights to in-scope systems are reviewed and approved. In case of exceptions identified, actions are taken to resolve the issue.	Inspected evidence of the core systems review and confirmed that the CTO reviewed and approved the users and their access permissions during the audit period. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0007	Annually, privileged access to the system is reviewed and approved by Management.	Inspected a list of users with privileged access to the network and infrastructure and confirmed this list was reviewed and approved by Management throughout the audited period. No exceptions noted.
		IS0154	Databases housing sensitive customer data are encrypted at rest (including on removable media such as backup tapes).	Inspected AWS RDS database settings and confirmed that databases are encrypted. Inspected AWS settings of data in transit to and from the system and confirmed data is encrypted with TLS certificate. No exceptions noted.
		IS0532	Data in transit is encrypted with SSL certificate	Inspected AWS settings of data in transit to and from the system and confirmed data is encrypted with TLS certificate. No exceptions noted.
		IS0861	Encryption keys used by integrated services are encrypted themselves with a unique master key. Access to encryption keys is restricted to authorized personnel only	Inspected the AWS key management system (KMS) to confirm that the company uses a system to manage encryption keys and keys are encrypted themselves with a unique master key. No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	IS0037	Access to in-scope components is managed by using a Role Based Access Controls (RBAC) mechanism	Inspected the primary account repositories of the system and confirmed that a Role Based Access Controls (RBAC) matrix is in place, detailing the entitlements for each account based on the relevant role. No exceptions noted.
		IS0040	A termination checklist is completed, and access is revoked for employees and external users as part of the termination process.	Observed a list of terminated employees, sampled employees who left the company during the audited period, obtained a clearance form for the sampled employees and confirmed that they were properly revoked from the company's systems. No exceptions noted.
		IS0097	Annually, access rights to in-scope systems are reviewed and approved. In case of exceptions identified, actions are taken to resolve the issue.	Inspected evidence of the core systems review and confirmed that the CTO reviewed and approved the users and their access permissions during the audit period. No exceptions noted.
		IS0007	Annually, privileged access to the system is reviewed and approved by Management.	Inspected a list of users with privileged access to the network and infrastructure and confirmed this list was reviewed and approved by Management throughout the audited period. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0473	In-scope system components require unique username and passwords (or authorized SSH keys) prior to authenticating users.	Inspected the mechanism used for user identification (in Okta) and confirmed that in-scope system users, including operating systems and databases, are identified through a user ID and a password. No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	IS0037	Access to in-scope components is managed by using a Role Based Access Controls (RBAC) mechanism	Inspected the primary account repositories of the system, and confirmed that a Role Based Access Controls (RBAC) matrix is in place, detailing the entitlements for each account based on the relevant role. No exceptions noted.
		IS0040	A termination checklist is completed and access is revoked for employees and external users as part of the termination process.	Observed a list of terminated employees, sampled employees who left the company during the audited period, obtained a clearance form for the sampled employees and confirmed that they were properly revoked from the company's systems. No exceptions noted.
		IS0473	In-scope system components require unique username and passwords (or authorized SSH keys) prior to authenticating users.	Inspected the mechanism used for user identification (in Okta) and confirmed that in-scope system users, including operating systems and databases, are identified through a user ID and a password. No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	IS0286	Access to AWS interface is restricted to authorized personnel only.	Inspected a list of users with access to AWS interface and confirmed this list was reviewed and approved by Management throughout the audited period. No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	IS0079	The company implements a Data Deletion policy which includes formal data retention and disposal procedures to guide the secure disposal of the company's and customers' data. The policy is reviewed and approved annually and available to the employees.	Inspected Unity's Security Policy, which details the data classification procedures, and confirmed that the policy refers to formal data deletion and disposal procedure to guide the secure disposal of the company's and customer's data. Confirmed that the policy was reviewed and approved by Management. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0115	Policies and procedures are in place to govern the retention of data.	Inspected Unity's Security Policy, which details the data retention procedures, and confirmed that the policy was reviewed and approved by Management. No exceptions noted.
		IS1100	All data deletion requests are documented, and a deletion certificate is retained for such requests.	Sampled examples of a data destruction requests and relevant certificates to confirm a data destruction process is in place upon customer's data deletion requests. No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	IS0649	Security Groups are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined.	Inspected AWS Security Groups settings to confirm that security settings are configured to limit unnecessary ports, protocols and services, and confirmed each open port is properly defined. No exceptions noted.
		IS0698	The system is automatically locked out for users after 6 invalid attempts.	Inspected Okta settings and confirmed that the system is locked after 6 invalid attempts. No exceptions noted.
		IS1330	Service account login credentials are stored in a password manager, and access to the credentials is restricted to authorized users with a business need.	Inspected the AWS Secrets Manager to confirm that privilege access to the password manager is limited to appropriate personnel. No exceptions noted.
		IS0474	Access to production environment requires two factor authentication.	Inspected the login configuration the production environment and confirmed that access to production requires 2 factor authentication (2FA). No exceptions noted.
		IS1224	Access to backed-up data and to the backup tool requires two factor authentication.	Inspected the login configuration the backup tool and confirmed that access to production requires 2 factor authentication (2FA). No exceptions noted.
		IS0481	Customers logging in from outside the system boundaries are required to authenticate with a username and a password, and a multi-factor authentication is enforced.	Inspected the login configuration the customer's environment and confirmed that access to production requires 2 factor authentication (2FA). No exceptions noted.
		IS0652	The company implements a Web Application Firewall system to detect and prevent application attacks outside from the system boundaries.	Observed the Firewall configuration to confirm a firewall is in place to protect against external threats, and to create separate segments in the internal network. No exception noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0949	Access to change settings in the Web Application Firewall is restricted to appropriate personnel.	Inspected the list of users with access to change settings in the firewall and confirmed access is limited to appropriate personnel. No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	IS0474	Access to production environment requires two factor authentication.	Inspected the login configuration the production environment and confirmed that access to production requires 2 factor authentication (2FA). No exceptions noted.
		IS1224	Access to backed-up data and to the backup tool requires two factor authentication.	Inspected the login configuration the backup tool and confirmed that access to production requires 2 factor authentication (2FA). No exceptions noted.
		IS0481	Customers logging in from outside the system boundaries are required to authenticate with a username and a password, and a multi-factor authentication is enforced.	Inspected the login configuration the customer's environment and confirmed that access to production requires 2 factor authentication (2FA). No exceptions noted.
		IS0473	In-scope system components require unique username and passwords (or authorized SSH keys) prior to authenticating users.	Inspected the mechanism used for user identification (in Okta) and confirmed that in-scope system users, including operating systems and databases, are identified through a user ID and a password. No exceptions noted.
		IS0861	Encryption keys used by integrated services are encrypted themselves with a unique master key. Access to encryption keys is restricted to authorized personnel only	Inspected the AWS key management system (KMS) to confirm that the company uses a system to manage encryption keys and keys are encrypted themselves with a unique master key. No exceptions noted.
		IS0668	The Anti-virus tool is configured to frequently scan for viruses, to get automated updates, and to prohibit users from disabling the tool.	Inspected the Crowdstrike Falcon tool settings and confirmed the tool scans threats automatically, is updated automatically with new threats, cannot be disabled by users and scans removable media before used. No exceptions noted.
		IS1305	A mobile device management (MDM) system is in place to protect against unauthorized removable media.	Inspected Bitlocker Endpoint Security settings to confirm the console configuration enforcing encryption for all removable and portable media devices. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
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.	IS0116	MDM software is implemented and maintained to provide for the interception or detection and remediation of malware.	Observed MDM system settings to confirm it is in place and manages mobile devices and endpoints against malware and security threats. No exceptions noted.
		IS0153	A mobile device management (MDM) system is in place to centrally manage mobile devices supporting the service.	Inspected the MDM tool settings and the list of mobile devices controlled by the tool to confirm that an MDM tool is in place and forced on endpoints used for accessing the system, in order to prevent or detect and act upon the introduction of unauthorized or malicious software. No exceptions noted.
		IS0667	Anti-virus technology is deployed for endpoints and is configured to be updated routinely, logged, and installed on all relevant production servers and endpoints.	Inspected the Crowdstrike Falcon tool settings and the list of endpoints controlled by the tool to confirm that an anti-virus software is installed on endpoints used for accessing the system, in order to prevent or detect and act upon the introduction of unauthorized or malicious software. No exceptions noted.
		IS0668	The Anti-virus tool is configured to frequently scan for viruses, to get automated updates, and to prohibit users from disabling the tool.	Inspected the Crowdstrike Falcon tool settings and confirmed the tool scans threats automatically, is updated automatically with new threats, cannot be disabled by users and scans removable media before used. No exceptions noted.
		IS0670	The Anti-virus tool is configured to send alerts in case of a potential virus discovery.	Inspected Crowdstrike Falcon settings to confirm that alerts are sent automatically to relevant personnel in case threats are identified. No exceptions noted.
		IS0673	Intrusion detection tools are used and configured to detect potential intrusions to the production environment. Alerts are sent automatically in case of a potential intrusion to relevant personnel.	Inspected the AWS Guard Duty tool used for intrusion detection and its settings to confirm it is in place and alerts in case of identified threats. No exceptions noted.
		IS0652	The company implements a Web Application Firewall system to detect and prevent application attacks outside from the system boundaries.	Observed the Firewall configuration to confirm a firewall is in place to protect against external threats, and to create separate segments in the internal network. No exception noted.
		IS0949	Access to change settings in the Web Application Firewall is restricted to appropriate personnel.	Inspected the list of users with access to change settings in the firewall and confirmed access is limited to appropriate personnel. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
	System Operations			
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	IS0002	The Company implements a baseline configuration for servers in order to define a standard level of service and security configuration for each server.	Inspected the configuration management tool to confirm that the company uses a baseline configuration in order to define a standard level of service and security configurations over the servers. No exceptions noted.
		IS0077	The Company maintains a server configuration and hardening policy for system components in-scope, with relevant configuration required to meet the company's objectives.	Inspected the Server Security Standard document and confirmed that it includes guidelines required for endpoints in the areas of security parameters, removal of unnecessary ports etc. No exceptions noted.
		IS0048	The Company utilizes a designated monitoring tool in order to enable activities investigation. The activities log is retained for 90 days.	Observed AWS CloudTrail system used by the company to confirm that the company monitors security and operation actions and user activity in the system. Observed log settings and confirmed the logs are retained for 90 days. No exceptions noted.
		IS0602	A SIEM tool is in place to alert when a sensitive activity or a security threat is identified.	Observed SUMO Logic configuration to confirm alerts are in place for critical activities such as login failures, capacity issues etc. No exceptions noted.
		IS0605	The Company utilizes a designated monitoring tool in order to enable activities investigation. The activities log is retained for 90 days.	Observed SUMO logic tool used by the company to confirm that the company monitors security and operation actions and user activity in the system. Observed log settings and confirmed the logs are retained for 90 days. No exceptions noted.
		IS0607	The monitoring tool provides a dashboard representing a timely, accurate and current data processed in the system.	Observed the SUMO logic tool's monitoring dashboard and confirmed it contains real time status of all the system components. No exceptions noted.
		IS0621	Access to the SIEM monitoring tool is restricted only to authorized personnel.	Observed SUMO Logic tool's login configuration and confirmed access to alter or change the tool is limited to appropriate personnel, and is password protected. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0668	The Anti-virus tool is configured to frequently scan for viruses, to get automated updates, and to prohibit users from disabling the tool.	Inspected the Crowdstrike Falcon tool settings and confirmed the tool scans threats automatically, is updated automatically with new threats, cannot be disabled by users and scans removable media before used. No exceptions noted.
		IS1305	A mobile device management (MDM) system is in place to protect against unauthorized removable media.	Inspected Bitlocker Endpoint Security settings to confirm the console configuration enforcing encryption for all removable and portable media devices. No exceptions noted.
		IS0009	The company has implemented a designated tool in order to identify new vulnerabilities before moving the change into the staging environments.	Inspected the tool used for code vulnerability scans and its settings to confirm the tool is in place and is set to review vulnerabilities in codes prior to deployment to production. No exceptions noted.
		IS0081	The company implements a Vulnerability Management policy which includes the scope and frequency of vulnerability identification activities and timelines for remediation.	Inspected the company's Application Security Vulnerability Management Procedure and confirmed that it details the scoping requirements, timelines, required remediation procedures, and relevant personnel who should perform the vulnerability scans. No exceptions noted.
		IS0544	In case of threats identified through a vulnerability scan, remediation tickets are created and prioritized according to their classification.	Inspected results of vulnerability scanning to confirm that tickets are created when vulnerabilities are identified, and prioritized according to their severity. No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	IS0081	The company implements a Vulnerability Management policy which includes the scope and frequency of vulnerability identification activities and timelines for remediation.	Inspected the company's Application Security Vulnerability Management Procedure and confirmed that it details the scoping requirements, timelines, required remediation procedures, and relevant personnel who should perform the vulnerability scans. No exceptions noted.
		IS0544	In case of threats identified through a vulnerability scan, remediation tickets are created and prioritized according to their classification.	Inspected results of vulnerability scanning to confirm that tickets are created when vulnerabilities are identified, and prioritized according to their severity. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0048	The Company utilizes a designated monitoring tool in order to enable activities investigation. The activities log is retained for 90 days.	Observed AWS CloudTrail system used by the company to confirm that the company monitors security and operation actions and user activity in the system. Observed log settings and confirmed the logs are retained for 90 days. No exceptions noted.
		IS0602	A SIEM tool is in place to alert when a sensitive activity or a security threat is identified.	Observed SUMO Logic configuration to confirm alerts are in place for critical activities such as login failures, capacity issues etc. No exceptions noted.
		IS0605	The Company utilizes a designated monitoring tool in order to enable activities investigation. The activities log is retained for 90 days.	Observed SUMO logic tool used by the company to confirm that the company monitors security and operation actions and user activity in the system. Observed log settings and confirmed the logs are retained for 90 days. No exceptions noted.
		IS0607	The monitoring tool provides a dashboard representing a timely, accurate and current data processed in the system.	Observed the SUMO logic tool's monitoring dashboard and confirmed it contains real time status of all the system components. No exceptions noted.
		IS0621	Access to the SIEM monitoring tool is restricted only to authorized personnel.	Observed SUMO Logic tool's login configuration and confirmed access to alter or change the tool is limited to appropriate personnel, and is password protected. No exceptions noted.
		IS0020	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected a database detailing the risk assessment work performed by the Company to confirm that it includes identified risks, owners and mitigation plans. Inquired about the identified risks to confirm they deem relevant to the system activity and environment. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0098	The board of directors meets quarterly and maintains formal meeting minutes. The board includes directors that are independent of the Company.	Observed sampled Board meetings presentations, and confirmed that the Board discussed items related to risks, controls, changes and mitigation activities where relevant. Confirmed that for the sampled Board meetings, meeting minutes were documented and shared with the Board members. Confirmed that some Board members are independent from Management. No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	IS0034	The Company has incident response procedures in place that includes an escalation plan based on the nature and severity of the incident to senior management, the board of directors and external parties as necessary.	Inspected the company's Incident Response Plan to confirm that the company has an incident response procedure in place. Confirmed that the document was properly approved by Management throughout the audited period. No exceptions noted.
		IS0098	The board of directors meets quarterly and maintains formal meeting minutes. The board includes directors that are independent of the Company.	Observed sampled Board meetings presentations and confirmed that the Board discussed items related to risks, controls, changes and mitigation activities where relevant. Confirmed that for the sampled Board meetings, meeting minutes were documented and shared with the Board members. Confirmed that some Board members are independent from Management. No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	IS0034	The Company has incident response procedures in place that includes an escalation plan based on the nature and severity of the incident to senior management, the board of directors and external parties as necessary.	Inspected the company's Incident Response Plan to confirm that the company has an incident response procedure in place. Confirmed that the document was properly approved by Management throughout the audited period. No exceptions noted.
		IS0098	The board of directors meets quarterly and maintains formal meeting minutes. The board includes directors that are independent of the Company.	Observed sampled Board meetings presentations and confirmed that the Board discussed items related to risks, controls, changes and mitigation activities where relevant. Confirmed that for the sampled Board meetings, meeting minutes were documented and shared with the Board members. Confirmed that some Board members are independent from Management. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
		IS0033	Incidents are logged, tracked, resolved, and communicated to affected parties by management. All events are evaluated to determine whether they could have resulted in a failure to meet the company's commitments and objectives.	Observed the ticketing system to confirm that incidents are logged, tracked, and communicated to affected parties by management until resolved
		IS0073	Security events are logged, tracked, resolved, and communicated to affected parties by management, according to the Company's security incident response policies and procedures. All events are evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives.	Inquired the company and observed the ticketing system and noted that no security incidents were identified by the company throughout the audited period. No exceptions noted.
		IS0072	The company performs a self-assessment to confirm the controls meet the organization's policies and operate effectively.	Observed controls matrices, lists of relevant procedures related to these controls, and internal test results, to confirm that the company assesses information required to support SOC 2 controls. No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	IS1225	Access to the backup scheduler is limited to appropriate personnel	Inspected a list of users with access to the backup scheduler and confirmed it is limited to appropriate personnel and was reviewed and approved by Management. No exceptions noted.
		IS0033	Incidents are logged, tracked, resolved, and communicated to affected parties by management. All events are evaluated to determine whether they could have resulted in a failure to meet the company's commitments and objectives.	Observed the ticketing system to confirm that incidents are logged, tracked, and communicated to affected parties by management until resolved
		IS0073	Security events are logged, tracked, resolved, and communicated to affected parties by management, according to the Company's security incident response policies and procedures. All events are evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives.	Inquired the company and observed the ticketing system and noted that no security incidents were identified by the company throughout the audited period. No exceptions noted.
	Change Management			
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data,	IS1098	Changes to software and infrastructure components of the service are formally documented, including their testing and approval.	Inspected the Jira system settings and several tickets to confirm the company has implemented designated a change management tool in order to manage, document, track and prioritize changes. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
	software, and procedures to meet its objectives.	IS0724	Branch protection rules are in place over code repositories to ensure deployments go through testing and approvals prior to deployments.	Inspected the automations related to pull request (PR) in GitHub to confirm the system forces a code review and sufficient tests prior to deployment to production. No exceptions noted.
		IS0009	The company has implemented a designated tool in order to identify new vulnerabilities before moving the change into the staging environments.	Inspected the tool used for code vulnerability scans and its settings to confirm the tool is in place and is set to review vulnerabilities in codes prior to deployment to production. No exceptions noted.
		IS0087	The Company has implemented a Software Development Life-Cycle policy that includes the role and responsibilities of each personnel, key milestones during the change management life cycle, unauthorized activities etc.	Inspected the company's SDLC policy to confirm that the policy is in place, available to relevant employees and was reviewed by Management. No exceptions noted.
		IS0105	The Company performs security impact analysis for changes as part of the Change Management process.	Inspected the system settings to confirm the system automatically forces a code review process where a different person approves the change before it can be merged. Inquired and were informed that as part of the code review, the reviewer performs a security impact analysis over the code change. No exceptions noted.
		IS0641	Tools are in place to retain prior versions of the system.	Inspected AWS ECR tool and confirmed images are retained with prior versions of the system. No exception noted
		IS1442	Changes to critical software and infrastructure components are logged with an audit trail to the relevant change tickets.	Inspected logs of changes, including changes to system components, network topology, firewall rule modifications, product upgrades and operating system upgrades to confirm a log is in place for all type of relevant changes, detailing the date and time of change. Confirmed the logs are properly retained and cannot be deleted. No exceptions noted.
	Risk Mitigation			
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	IS0020	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected a database detailing the risk assessment work performed by the Company to confirm that it includes identified risks, owners and mitigation plans. Inquired about the identified risks to confirm they deem relevant to the system activity and environment. No exceptions noted.

TSC Ref. #	Criteria	Control Number	Control Description	Test Results
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	IS0020	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected a database detailing the risk assessment work performed by the Company to confirm that it includes identified risks, owners and mitigation plans. Inquired about the identified risks to confirm they deem relevant to the system activity and environment. No exceptions noted.
		IS0068	The Company's Organization Structure and Reporting lines are updated regularly. The Organization Structure and Reporting lines' information is available for employees through HR systems.	Inspected the company's Organizational Chart and confirmed it details the roles and the reporting channels of the company. Confirmed that the Organizational Chart was approved by Management throughout the audited period. No exceptions noted.
		IS0071	Formal policies and procedures that outline the requirements for vendor management are documented and include the following components: Maintaining a list of critical vendors, Requirements for critical vendors to maintain their own security practices and procedures, annually reviewing attestation reports for critical vendors or performing a vendor risk assessment.	Inspected a database detailing the vendor risk assessment work performed by the Company to confirm that it includes identified risks, owners and mitigation plans. No exceptions noted.
		IS0124	Periodically, Management assesses critical third-party vendors to confirm they comply with security commitments and requirements.	Inspected a database detailing the vendor risk assessment work performed by the Company to confirm that it includes identified risks, owners and mitigation plans. No exceptions noted.
		IS1282	Before contracting with a new vendor, Management verifies that the agreement with the new vendor includes a NDA and confidentiality requirements, as well as an acknowledgement of the Code of Conduct.	Sampled critical vendors to confirm that the sampled vendors signed on a non-disclosure agreement (NDA). No exceptions noted.
		IS0029	The Company has implemented a vendor management policy, which details the procedures to assess the vendor's performance, address issues with the vendor's performance, terminating relationships with vendors and assessing the vendor's compliance with the Company's requirements.	Inspected the company's Vendor Management Policy to confirm that there is a vendor management process in place. Confirmed that the policy was reviewed and approved by Management throughout the audited period. No exceptions noted.