Preservica, Inc.

System and Organization Controls (SOC) 2 Type II Report

October 1, 2021 to September 30, 2022

255 STATE STREET, BOSTON, MA 02109
P: 617.439.9700

WOLF
& COMPANY, P.C.

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITOR'S REPORT 1

II. ASSERTION OF PRESERVICA, INC.'S MANAGEMENT 6

III. DESCRIPTION OF PRESERVICA, INC.'S SYSTEMS 8

A. SYSTEM OVERVIEW 8

B. INFRASTRUCTURE 9

C. SOFTWARE 9

D. PEOPLE 10

E. PROCEDURES 11

F. DATA 12

G. OTHER RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESSES, INFORMATION AND COMMUNICATION SYSTEMS, AND MONITORING CONTROLS 13

H. CHANGES TO THE CONTROL ENVIRONMENT 21

I. TRUST SERVICES CRITERIA NOT APPLICABLE TO THE IN-SCOPE SYSTEM 21

J. APPLICABLE TRUST SERVICES CRITERIA AND RELATED CONTROLS 22

K. COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS 22

L. COMPLEMENTARY USER ENTITY CONTROLS 24

IV. INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS 25

A. INTRODUCTION 25

B. APPLICABLE TRUST SERVICES CRITERIA 25

C. TESTING OF OPERATING EFFECTIVENESS 26

V. ADDITIONAL INFORMATION PROVIDED BY PRESERVICA, INC. 85

A. CONTROL EXCEPTIONS AND PRESERVICA, INC.'S MANAGEMENT RESPONSES 85

I. INDEPENDENT SERVICE AUDITOR'S REPORT

To: Preservica, Inc.

Scope

We have examined Preservica, Inc.'s (Preservica's) accompanying description of its system titled "Description of Preservica, Inc.'s System" throughout the period October 1, 2021 to September 30, 2022 (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 the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Preservica's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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*).

Preservica uses subservice organizations to support the operation of the system. Preservica uses Amazon Web Services (AWS) and Microsoft Azure to provide cloud infrastructure. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Preservica, to achieve Preservica's service commitments and system requirements based on the applicable trust services criteria. The description presents Preservica's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Preservica's controls. The description does not disclose the actual controls at the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Organization's Responsibilities

Preservica 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 Preservica's service commitments and system requirements were achieved. Preservica has provided the accompanying assertion titled "Assertion of Preservica, Inc.'s Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Preservica 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 Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of 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 (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 and operated 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.

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.

Controls Did Not Operate During the Period Covered by the Report

The description discusses the following controls; however, during the period of October 1, 2021 to September 30, 2022 the controls did not operate for the applicable criteria:

Key	Service Organization Controls	Test
CC7.5.4b A1.2.1b	Appropriate personnel are notified of failures or errors during the backup process for investigation.	Inquired with management to confirm there were no AWS backup failures to verify appropriate personnel are notified during the audit period. Therefore, the Service Auditor was unable to test the operating effectiveness of the control during the audit period.
CC8.1.8b	Emergency change requests are verbally approved and will be documented after the fact.	Inquired with management to confirm there were no emergency changes during the audit period. Therefore, the Service Auditor was unable to test the operating effectiveness of the control during the audit period.

Description of Tests of Controls

The specific controls we 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 Preservica's system that was designed and implemented throughout the period October 1, 2021 to September 30, 2022, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Preservica'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 organizations and user entities applied the complementary controls assumed in the design of Preservica's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Preservica's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Preservica'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 Preservica, user entities of Preservica's system during some or all of the period October 1, 2021 to September 30, 2022, business partners of Preservica 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:

- 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.

Wolf & Company P.C.

Boston, MA
October 12, 2022

II. ASSERTION OF PRESERVICA, INC.'S MANAGEMENT

We have prepared the accompanying description of Preservica, Inc.'s (Preservica's) system titled "Description of Preservica, Inc.'s Systems" throughout the period October 1, 2021 to September 30, 2022 (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 report users with information about the system that may be useful when assessing the risks arising from interactions with Preservica's system, particularly information about system controls that Preservica 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 and availability (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*).

Preservica uses subservice organizations to support the operation of the system. Preservica uses Amazon Web Services (AWS) and Microsoft Azure to provide cloud infrastructure. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Preservica, to achieve Preservica's service commitments and system requirements based on the applicable trust services criteria. The description presents Preservica's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Preservica's controls. The description does not disclose the actual controls at the subservice organizations.

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

Controls Did Not Operate During the Period Covered by the Report

The description discusses the following controls; however, during the period of October 1, 2021 to September 30, 2022 the controls did not operate for the applicable criteria:

Key	Control Activity	Reasons Control Did Not Operate
CC7.5.4b A1.2.1b	Appropriate personnel are notified of failures or errors during the backup process for investigation.	No AWS backup failures occurred during the audit period.

Key	Control Activity	Reasons Control Did Not Operate
CC8.1.8b	Emergency change requests are verbally approved and will be documented after the fact.	No emergency changes occurred during the audit period.

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

a. the description presents Preservica's system that was designed and implemented throughout the period October 1, 2021 to September 30, 2022, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Preservica'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 organizations and user entities applied the complementary controls assumed in the design of Preservica's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Preservica's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Preservica's controls operated effectively throughout that period.

III. DESCRIPTION OF PRESERVICA, INC.'S SYSTEMS

A. SYSTEM OVERVIEW

Preservica, Inc. (Preservica or the Company) supplies digital preservation software as cloud-based Software-as-a-Service (SaaS) to support customers in the cultural heritage, education, corporate and public sectors worldwide.

Following initial research around 2000, Preservica's software technology has been in continuous development. Since 2003, the technology has grown from a one-off project, to a template for bespoke developments, to an off-the-shelf product. In December 2015, Preservica split from its parent Company and has been trading as an independent Company ever since. In that time, the customer base has grown to over three hundred fifty (350) organizations with users in over ninety (90) countries and includes national archives and libraries, regional archives, academic archives and libraries, large museums, and corporates. In addition, the Company has over 3,400 freemium users using the new Starter Edition.

The Company's products are delivered as a portfolio of SaaS solutions, including the following:

Starter Edition	For smaller collections and institutions. Available fully hosted on Amazon Web Services (AWS) multi-tenant.
Essentials & Professional Editions	For small to medium collections needing more advanced functions. Available fully hosted on AWS multi-tenant.
Enterprise Edition	For large collections where high levels of performance and security are paramount. Available fully hosted as dedicated private cloud (single-instance) on either AWS or Microsoft Azure.
Enterprise On Premise Edition	For larger collections and institutions. Installed, run and managed in-house.

Preservica's software development is controlled via a Product Management Board. There is no customized development, however, the Company will undertake customer-sponsored development providing it is a standard feature.

B. INFRASTRUCTURE

Preservica utilizes AWS and Microsoft Azure as its infrastructure provider and solutions partner to support scalability, availability and durability of the platform and services. SaaS products are hosted in AWS regions located in the United States of America, Canada, Australia, and Ireland and in Azure regions located in West Europe, UK South and East USA.

Preservica is an AWS Advanced Technology Partner which provides additional benefits for marketing and selling Preservica including Marketing Development Funds. Preservica has achieved both AWS ISV Government Competency and AWS Education ISV Competency, through demonstrating the highest level of specialization, deep AWS technical expertise, and proven customer success.

Preservica also partners with Microsoft where as an ISV Co-sell ready Partner. In addition, the Company is part of Microsoft's ISV Success Program and also a member of its Content Services Partner Program, with the latter program being by invite only.

Additionally, Preservica has partnered with TechData to host its software on the Microsoft Azure platforms both in the United States of America and the United Kingdom.

C. SOFTWARE

The Preservica product software is written in Java. The in-scope infrastructure consists of multiple applications and services as shown in the table below:

Component	Description
Build, release and continuous integration systems	• Repository Manager – BitBucket • Source Code Version Control – BitBucket • Release Management Tool – TeamCity • Automated Continuous Integration – TeamCity • Build Management and Continuous Integration Service – TeamCity
Hosting Systems	• AWS Environment • Microsoft Azure Environment
Databases and Storage	• mySQL Database • Simple Storage Service (S3) and Elastic File System (EFS) in AWS • Blob and File Storage in Azure

Network Infrastructure	*AWS* • Virtual Private Cloud (VPC) • Security Groups • Application Load Balancers • NAT Gateway for Outgoing Traffic *Azure* • Virtual Network • Network Security Group • Application Gateway
Monitoring Systems	• Telegraf • Uptime Robot *AWS* • CloudWatch • CloudTrail *Azure* • Monitor
Key Management	*AWS* • KMS • S3 Key Management Service *Azure* • Storage Service Encryption

D. PEOPLE

Preservica employs approximately ninety (90) staff who are organized in the following functional areas of Corporate, Engineering, Innovation, Product Management, Operations, Support, Sales, Partners and Marketing. The Company has approximately an additional thirty (30) outsourced staff in Engineering. All outsourced staff are required to follow the information security policies and procedures, sign a document at induction and again on an annual basis stating they have read and understood the required documents.

- **Corporate** – Consisting of the Chief Executive Officer (CEO), Chief Financial Officer (CFO), Assistant Chief Financial Officer, finance, human resources, quality, and information security. The CEO determines the strategy in line with the Board and Leadership Team, communicates this to all employees and outsourced teams and ensures the strategy is delivered. The CFO and other corporate staff provide financial information, compliance with quality and information security standards and human resource requirements including recruitment, training and rewards.

- **Engineering** – The Chief Technology Officer (CTO) leads the Engineering function defining the long-term technical architecture and technology strategy of the product and deployment of the product to the operations team. This team consists of Lead Engineers and teams of Software Engineers, Test Department, DevOps plus an outsourced team of Software Engineers.
- **Innovation -** The Chief Innovation Officer (CIO) leads the innovation team to deliver proof of concepts exploring new approaches to the way the product is used and exploited.
- **Product Management** – The Chief Product Officer (CPO) works with the Leadership Team to define the product strategy, devising and articulating the product roadmap and ensuring the engineering team have sufficient information to develop the product. The team consists of the VP Product Management, Product Owners and UX Design.
- **Operations** – The Operations Director oversees internal systems, cloud operations (responsibility for deployment and maintenance of the product on AWS and Microsoft Azure platforms and on-premise solutions) and the customer experience team (managing customer requirements and expectations and ensuring customer engagement success).
- **Support** – The Customer Success Manager oversees the service desk / support team and the Training Manager who provide on-boarding for new customers and support through the Company's ticketing system to deal with issues, ensuring Preservica achieves its service level agreements.
- **Marketing, Partners and Sales** – These departments help define the strategies for developing market and commercial opportunities to grow revenues and lead to sustainable revenue. This is achieved through building new business channels, expanding the Company's partnerships in existing geographies and recruiting new partners to enable Preservica to enter new geographical markets. Preservica's sales team engages directly with its customer to sell the full range of products into key target markets across the globe.

E. PROCEDURES

Preservica maintains a Quality Management System (QMS) (ISO 9001) and Information Security Management System (ISMS) (ISO 27001) on SharePoint or Confluence to ensure that policies and procedures are:

- Properly communicated throughout the organization
- Properly owned, managed and supported
- Clearly outlined business objectives
- Focused on continual iteration and improvement
- Showing commitment to meet regulatory obligations
- Supported by the Structure Document

These procedures cover the following key information security areas:

- Maintenance of restricted access to system configurations, functionality, master passwords and security devices (e.g. firewalls)

- Maintenance and support of the security system and necessary backup and storage
- Selection, documentation and implementation of security controls
- Categorization of information relating to information assets
- Management of access and roles
- Monitoring security controls
- Incident response

All new staff are inducted into the Target Operating Model (TOM),comprising of the Quality Management System and the Information Security System. Additionally, all staff undergo annual refresher training on key information security policies and procedures.

F. DATA

All Preservica employees share in the responsibility to safeguard information with an appropriate level of protection by observing the information classification policy:

- Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification
- Do not label information but store the documents in different SharePoint locations depending on their classifications
- Access to information is restricted depending on the type of protection required and recorded in the User Access Control Record
- Manage all removable media with the same handling guidelines as below
- Media being disposed of should be securely deleted
- Media should be protected against unauthorized access, misuse or corruption during transportation

The following guidelines are used to classify data at Preservica:

Rating	Description	Availability
Public	Disclosure causes no harm	Available to all interested parties
Internal	Disclosure causes minor embarrassment or minor operational inconvenience	Available to all employees
Restricted	Disclosure has a serious impact on long term strategic objectives or put eh survival of the organization at risk	Available to limited employees or trustees that are directly involved with the asset or application

Confidential	Disclosure has a significant short-term impact on operations or tactical objectives	Strictly between people who have access to the assets

G. Other Relevant Aspects of the Control Environment, Risk Assessment Processes, Information and Communication Systems, and Monitoring Controls

1) Control Environment

Management Philosophy

The Board and management of Preservica are committed to preserving the confidentiality, integrity and availability of all physical and electronic information assets throughout the organization and the control environment reflects this philosophy.

Preservica recognizes that information security is key to the success of the business. Within operations, the Company aims to prevent and minimize the impact of security incidents in order to enhance their reputation and support business growth in line with its strategic direction. To support this aim, Preservica has implemented an Information Security Management System (ISMS) which complies with the ISO27001:2013 standard.

The Preservica Governance Charter provides details and membership of the various sub committees and boards. The Board of Directors retains full responsibility for overseeing and appraising Preservica's strategies, policies, performance and governance framework. The Board comprises Directors who bring a mix of skills, knowledge, experience, diversity and independence, together with a deep understanding of and competence to deal with current and emerging issues to guide the business.

The CEO, CFO, and the CIO serve as the link between the Board and the remainder of the Leadership Team. The Leadership Team has representation from all business areas and serves as the decision-making body of the Company. The Leadership Team meets every week to discuss operational matters for prompt decision making and implementation and monthly to deal with future strategic aims. The Leadership Team is responsible for ensuring the business is executing the strategy agreed with the Board.

The Leadership Team with support from the Information Security Manager and the IT security Manager are responsible for the ISMS. This group meets annually to review and set appropriate goals for information security and to undertake a review of the Company's Risk Register.

The importance of security in Preservica is emphasized through the establishment and communication of policies and procedures, investment in resources, a rigorous induction program for new staff and annual security refresher training for all staff. The induction and refresher training also applies to contract staff working on the product.

Senior Management are involved in all aspects of information security including:

- Standards – Preservica follows specific standards in the development of its product that enables us to exercise practices around security, availability, quality, reliability and confidentiality.
- Tools – Preservica uses tools to effectively communicate and collaborate to help ensure activities and issues are properly tracked.
- Risk Monitoring – Preservica maintains a corporate risk register and considers both internal and external risks that could affect the business.

Integrity and Ethical Values

Preservica's integrity and ethical values are essential as the control environment is ultimately dependent on the employees who design, operate and monitor the various components in order to make them effective.

The Code of Conduct outlines the way in which Preservica does business and is underpinned by policies including equality and diversity, anti-bribery and corruption, fraud and work health and safety.

Organizational Controls

Security Management – For the purpose of managing the ISMS, an Information Security Manager (ISM) has been appointed who will ensure that non-compliances and exceptions will be handled as defined in the ISMS procedures. The ISM is responsible for ensuring Preservica's policies and procedures are maintained and enforced. The Information Security Policy is reviewed annually by the ISM and signed off by the CEO. All staff are required to read the policy on an annual basis.

Incidents are managed using Preservica's risk management process. This process ensures the Company continually monitors and mitigates risks to the business operation. It also produces and maintains the corporate risk register, ensuring it is up to date and effectively managed. All information security risks are allocated an owner and allocated an impact value by reference to confidentiality, availability and integrity.

Updates to policies and procedures are communicated to staff as new versions are released. All new employees are required to read certain mandatory security policies and procedures on starting employment. An annual refresher course is also mandatory for all employees.

Security Policies – The following security policies and procedures are in place for Preservica:

- Data classification and Management
- Risk management and treatment

- Selection, documentation and implementation of security controls
- User access authorization and removal
- Monitoring of security controls
- Incident management

Personnel Security – Preservica operates a rigorous recruitment process for all new members of staff. Roles and responsibilities are documented in the job ad/description as well as required education and experience. Each applicant undergoes a process involving interviews with senior members of the organization.

Successful candidates are required to sign an employment agreement with the Company which includes clauses for maintaining confidentiality and non-disclosure of information.

Background and passport verification checks are used to ascertain a candidate's previous employment, criminal record and right to work. References must cover the prior three (3) years any gaps in employment or education must be covered by a personal reference who must not be a family member. Background checks include the following:

- Address verification
- Credit reference check
- Federal and county court search for US based staff (depending on the job role)
- Disclosure and barring service report for UK based staff (depending on the job role)
- Sanctions list check

All staff with potential access to customer data must undergo a Criminal and County Court search (US staff) or a Disclosure and Barring Service report (UK staff). This is repeated annually.

On termination, the Internal Systems team complete the Leaver IT Procedure including removing access to systems, return of Company equipment, and updating the User Access Control record. An interview with HR personnel is also held to confirm leaving date, any monies due and to obtain feedback on their employment and reasons for leaving.

Preservica's information security incident management procedure is a key document and therefore subject to annual review by all staff. Staff are required to immediately inform the CEO or CFO, their manager and the Information Security Manager regarding any information security event or suspected event.

Change Management – Change management policies and procedures are maintained and define the process for the management of changes to systems and applications in production. Change can arise resulting from a number of triggers including new software or configuration change requirements to improve throughput, security, or availability.

The Change Advisory Board (CAB) approves or denies requests based on the holistic view of all change being considered for any given period. The CAB consists of the Cloud Operations team with the Change Manager role being fulfilled by the Operations Director and they meet on a weekly basis.

All change requests are logged, tracked in the ticketing system, and categorized into the following types:

- **Standard Change -** A change which has been done several times in the past, is considered low risk and impact and can be executed without formal approval. All standard changes are reviewed at the weekly meeting.
- **Normal Change -** A normal change requires approval at the weekly CAB meeting and are considered in terms of volume of change required, availability of resources, risk assessment, and security impact.
- **Emergency Change -** A change that needs to be implemented with urgency to resolve or prevent a degradation in service availability. Approval should be sought from the Change Manager or other members of the CAB immediately.

Preservica has a well-defined and formalized systems development methodology that includes project planning, design, testing, implementation, and maintenance. During sprint planning, the Engineering team will commit to a number of work items to be completed during the upcoming sprint which is a 2-week process. Senior Engineers from each Engineering team along with the DevOps Manager, Software Architect, and an Ops representative will hold a technical review to discuss and peer review any changes that are being planned and any impact on operations. Once the sprint is concluded all the teams meet to demonstrate functionality and discuss any improvements to the process. The sprint is signed off following a demonstration of the completed stories to Product Management.

On completion of the sprint, the code is passed to the Test Department for manual and automated testing. Testing includes user centric tests, compatibility and lifestyle testing, security, and performance testing. Regression tests are also run to verify that the existing product functionalities are working correctly even after they were changed or interfaced with other software.

Release versions are retained and mapped within the version control, and build / release management. This allows for individual software changes to be easily rolled back should unexpected behavior be observed prior to release. Software releases can be rolled back to the last stable release or patch prior to a given release being used in a live production environment.

Data Back Up and Recovery

- **Storage (Amazon)** - Preservica software uses Amazon S3 (Amazon Simple Storage Solution) which is a data storage infrastructure for the storage of objects logically organized into buckets. Amazon S3 durability is achieved through synchronously storing objects across multiple regions before confirming that the data has been successfully stored. Amazon S3 calculates checksums on all networks traffic to detect corruption of data packets when sorting or retrieving data. It also performs regular, automatic data integrity checks. S3 and Glacier buckets are not backed up. Preservica relies on AWS' durability commitment. Furthermore, customers' S3 and Glacier long term storage buckets are protected from accidental deletion by a series of security measures such as multi-factor authentication (MFA) and versioning.
- **Storage (Microsoft)** - Microsoft Azure stores multiple copies of the data and is protected from planned and unplanned events including transient hardware failure, network or power outages, and natural disasters. Redundancy ensures the data storage account meets its availability and durability commitments even in the face of failures. Data in an Azure Storage account is replicated three (3) ways in the primary region using zone redundant storage (ZRS), which copies data synchronously across the Azure availability zones in the primary region.
- **Business Continuity Planning** - Preservica maintains a Business Continuity Plan designed to minimize the impact of adverse events on the business. The Plan addresses multiple levels of business continuity ranging from staff succession planning to disaster recovery. Preservica's business continuity plans are reviewed, tested, and approved on an annual basis.
- **Disaster Recovery Planning** - Preservica maintains thirty (30) daily backups for mySQL server to enable recovery to any point in time from the past month and a single monthly backup is maintained for up to one (1) year. Following major updates to the system, including security and kernel upgrades, personnel changes, and major tool additions, Preservica maintains a virtual machine image from the last major upgrade. The viability of the backups is tested on a regular basis to confirm they would be available as needed in the event of a disaster.
- **Site Reliability** - Cloud Operations Team use automated monitoring and alerting tools to detect outages in the platform, database, or application and any outage triggers the Incident Response Plan. The Team utilizes a number of tools for monitoring the site, which includes tools for managing, recording incidents, and post-mortem management. The Team focuses on learning and continuous improvement by sharing information with incident owners and senior managers.
- **Environmental Controls** - The production environments are fully hosted on Amazon Web Services and Microsoft Azure.

System Account Management

Production Environment Access

Customer Access

Preservica will provision a tenancy for a customer and create at least one (1) user with the appropriate role, who can then create other users, as needed. The account credentials will be sent to each individual user via email. Customers are responsible for managing access to their own tenancy.

Preservica Internal Users Access

Access to the Preservica production environments is strictly controlled and only provisioned to appropriate staff from the Operations department. Access is only possible from the Preservica internal network or while connected to the corporate Virtual Private Network (VPN). Users can also only gain access to production servers via SSH, with a valid key, through a jumpbox, which further enhances security and segregation.

Password Requirements

Customer Access

The password settings for Preservica cloud editions are governed through password complexity and passwords must be at least eight (8) characters long and require three (3) of the following: lowercase letters, uppercase letters, numbers or symbols (special characters). Customers can also enable MFA on their tenancy and certain editions can be linked to a customer's existing Identity Provider with SAML (Security Assertion Markup Language).

Preservica Internal System Access

Wherever possible, Preservica uses its local Active Directory or synchronized Azure Active Directory to provide access to systems used by the Company. Password complexity requirements are set in Active Directory. Where a system cannot be accessed by single sign on (SSO), or the Company's password policy requirements cannot be enforced by the system, users must follow the guidance given in the password policy when creating passwords.

User Provisioning, De-provisioning and Review of Preservica Internal Users

User provisioning and de-provisioning is initiated via an internal helpdesk with requests being made by HR or a user's line manager. Users are only given access to systems and resources that are required to carry out their job and the principals of role-based access and least privilege are followed.

Access to systems is granted and removed by a user administrator of the system who will also review who has access to the system at least every six (6) months.

If a user changes roles within the organization then their access to systems will be reviewed to make sure they have access to the appropriate systems at the appropriate level for their new role.

2) Risk Assessment Processes

Preservica has a business wide risk management framework that is managed by the Quality Manager.

A key component of this framework is the development and maintenance of a Corporate Risk Register, which is regularly reviewed by the Leadership Team. Potential risks to the business are assessed across key risk categories, which include reputational, commercial, product, operations, human resources, financial, compliance, and other. This is reviewed by the Leadership Team at least annually to ensure the risks remain within the desired risk appetite and if not, mitigated with further actions put in place to reduce the risk.

In order to manage information security risks, processes are in place for identification, assessment, and treatment of these risks. An ISMS Assets Risk Management Register is used to record the details of the risk, vulnerabilities, and deficiencies to ensure they can be assessed, the risk to Preservica understood, and appropriate mitigation or treatment determined. The risk assessments determine the potential threat which could exploit the vulnerability and the probability and impact of this occurring. This is reviewed by the Leadership Team at least annually and updates to control activities and information security policies are performed as necessary.

All security risks are allocated to a Risk Owner. Risks exceeding the tolerance limit set by the Company must be considered for additional mitigation and action to reduce the risk. During risk treatment, asset owners must consider the following options:

- Accept risk
- Monitor risks and consider improving controls
- Significant risks: monitor risks, consider treatment
- Critically significant risks: plan risk treatment

Individual vulnerabilities in Preservica product code are separately managed using a ticketing system and assigned to the appropriate product team for remediation. A security priority is agreed by either the Preservica Bug Board or the Technical team and this dictates the remediation time frame. Remediation progress is tracked in the ticketing system.

Preservica engages with an external consultancy on an annual basis to perform a penetration test on the Preservica digital preservation software. This report is made available to key members of the Leadership Team and action is taken where appropriate to address any issues highlighted by the report.

Preservica also engages external auditors to perform compliance audits on a regular basis relating to our ISO: 27001 and ISO: 9001 certifications. The results of these audits are captured and reported on an improvement register.

Preservica has a formal framework for managing the lifecycle of key ISMS supplier relationships, including how the Company assesses and annually monitor the relationships. As part of the supplier onboarding process, key suppliers are subject to a selection process including a review of any information security requirements and a privacy impact assessment, if deemed necessary. Supplier agreements, including terms and conditions are also reviewed and signed prior to engaging with any supplier. Additionally key suppliers are evaluated on an annual basis for ongoing compliance to their contractual obligations. Key documents including SOC 2 reports, ISO: 27001 and ISO: 9001 certifications and credit reports are collated, where possible, and made available for review by the supplier owner.

A whistleblowing policy exists and is available to all staff. This policy is included in both the induction list of policies and procedures which are mandatory reading for all new staff upon hire and annually by all other employees.

3) Information and Communication Systems

Internal Communication

Preservica maintains communication with employees using email, tools such as Microsoft (MS) Teams, internal knowledge bases, and global employee meetings. This communication includes but is not limited to annual strategy and quarterly business reviews, new product features, market updates, publication of policies and procedures, awareness, and training.

Policies and procedures specific to operations, including those for managing security are made available to all staff and contractors on the internal system. Changes and updates are communicated via email.

All employees, and where appropriate, contractors, receive appropriate awareness education and training on organizational policies and procedures, as relevant to their role.

External Communication

Preservica uses its website, blog, email, social media and user group portal to communicate to external customers, vendors and other parties.

Customer responsibilities and terms of use are stated in the customer contract.

Non-disclosure agreements and contracts are signed by third parties prior to confidential information being shared with those parties.

4) Monitoring Controls

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities and evaluation.

A regular review and evaluation of Preservica's ISMS provide the Board, the Leadership Team, and customers with assurance Preservica conforms with the ISO 27001 standard. It will also identify any omissions or weaknesses. This is achieved by conducting audits and reviews of:

- Security management activities i.e., governance, risk management
- Security documentation e.g., policies, procedures
- Implemented controls

Ongoing Monitoring

Preservica uses a wide range of automated and manual monitoring systems which cover security, service performance, and availability. Monitoring tools are implemented to detect and trigger alerts of external and internal threats. The availability and capacity of AWS and Microsoft Azure environments are also continuously monitored through a specific set of tools and control procedures.

5) Customer Support

A dedicated Customer Support team is in place to service customer requests and monitor customer feedback on performance issues. These issues are communicated to the Cloud Ops and Engineering teams for resolution. Customers are able to file their own support tickets through Preservica's service desk platform.

H. Changes to the Control Environment

Preservica is required to disclose relevant detail of changes to the system during the period covered. There were no changes to the control environment supporting the system during the covered period.

I. Trust Services Criteria Not Applicable to the In-Scope System

The trust services criterion presented below is not applicable to Preservica's system. As a result, associated controls are not required to be in place at Preservica for the not applicable trust services criterion.

Criteria	Reason Criteria is Not Applicable
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.	This criterion is not applicable as Preservica's system is hosted within AWS and Microsoft Azure and data is not saved on any employees' laptops. Therefore, Preservica has no responsibilities to restrict access to facilities and physical assets supporting the system.
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.	This criterion is not applicable as Preservica's system is hosted within AWS and Microsoft Azure and data is not saved on any employees' laptops. Therefore, Preservica has no responsibilities to discontinue the use of physical assets supporting the system.

J. APPLICABLE TRUST SERVICES CRITERIA AND RELATED CONTROLS

The applicable trust services criteria and Preservica's controls are included in section IV of this report, *Independent Service Auditor's Description of Tests of Controls and Results*, to eliminate the redundancy that would result from listing them in this section and repeating them in section IV. Although the applicable trust services criteria and related controls are included in section IV, they are, nevertheless, an integral part of Preservica's description of systems.

K. COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

Preservica uses subservice organizations to perform various functions to support the delivery of services to user entities. Preservica has risk rated the subservice organizations and performs monitoring activities to ensure the subservice organizations have the necessary internal controls. Monitoring includes the receipt and review of the subservice organizations' internal audit reports (e.g. SOC 2 Reports).

The following is a description of the subservice organizations used by Preservica to support the delivery of systems:

Amazon Web Services (AWS): Provides cloud infrastructure for the servers used to store data along with other network components.

Microsoft Azure: Provides cloud infrastructure for the servers used to store data along with other network components.

The following applicable trust services criteria are intended to be met in part by complementary subservice organization controls implemented by the subservice organizations including, but not limited to, the following:

Criteria	Complementary Subservice Organization 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.	AWS and Microsoft are responsible for monitoring, evaluating, communicating, and correcting of network and perimeter security, performance, events on the production servers.
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.	AWS and Microsoft are responsible for implementing physical security controls to restrict access to their data centers and protected information assets supporting the cloud infrastructure to authorized personnel.
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.	AWS and Microsoft are responsible for data wiping, destroying, and disposing of assets supporting the cloud infrastructure that are no longer required or have reached end of life.
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.	AWS and Microsoft are responsible for monitoring their environments supporting the cloud infrastructure to maintain security and availability, including having an incident handling 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.	AWS and Microsoft are responsible for developing and implementing a change control process that requires formal request, documentation, testing, approval, and implementation.

Criteria	Complementary Subservice Organization Controls
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	AWS and Microsoft are responsible for developing, implementing, maintaining, and monitoring environmental protections of the assets hosted in their data centers supporting the cloud infrastructure.
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	AWS and Microsoft are responsible for implementing and testing recovery plan procedures to meet availability objectives.

L. COMPLEMENTARY USER ENTITY CONTROLS

Preservica's operations were designed with the assumption that certain controls would be placed in operation by user entities (customers). This section describes the controls that should be in operation at user entities to complement the controls at Preservica. User auditors should determine whether user entities have established controls to provide reasonable assurance over the following:

1. Customers are responsible for configuring their own Preservica instance, including the appropriate set-up of their logical security such as user accounts, passwords, and MFA.
2. Customers are responsible for managing access rights, including privileged access.
3. Customers are responsible identifying approved points of contacts to coordinate with Preservica.
4. Customers are responsibility for the security and confidentiality of the data submitted on Preservica support tickets.
5. Customers are responsible for requesting and monitoring Preservica's customer support access to their account.
6. Customers are responsible for requesting their tenancy to be removed.
7. Customers are responsible for alerting Preservica on incidents (related to security and availability) when they become aware of them.
8. Customers are responsible for the security of the data prior to import and ongoing monitoring after data has been uploaded.
9. Customers are responsible for ensuring that their machines, devices, and network are secure.
10. Customers are responsible for assessing and evaluating any potential impact add-ons may have on their instance.

IV. INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

A. INTRODUCTION

This section presents selected information provided by Wolf & Company, P.C. This information includes:

- A description of tests performed by Wolf & Company, P.C. to determine whether Preservica's controls were operating with sufficient effectiveness to meet the applicable trust services criteria; and
- Results of Wolf & Company, P.C. tests of operating effectiveness.

Also included in this section is information provided by Preservica's management. This information includes:

- The applicable trust services criteria as set forth in TSP Section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*); and
- Description of controls implemented by Preservica to meet the applicable trust services criteria.

B. APPLICABLE TRUST SERVICES CRITERIA

The applicable trust services criteria in scope and controls to meet the applicable trust services criteria were provided by Preservica's management. While this information is provided by Preservica, it is more beneficial to have it reported in section IV (*Independent Service Auditor's Description of Tests of Controls and Results*) to facilitate the report of tests of controls and results of testing which is provided by Wolf & Company, P.C. The following trust services criteria were in scope.

- **Security Criteria** – Information and systems are 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 entity's ability to meet its objectives.
- **Availability Criteria** – Information and systems are available for operation and use to meet the entity's objectives.

C. TESTING OF OPERATING EFFECTIVENESS

Key	Service Organization Controls	Tests	Results
CC1.0 - Control Environment			
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1a	Employees are required to acknowledge the Employee Terms and Conditions Agreement upon hire.	Inquired with management to confirm employees are required to acknowledge the Employee Terms and Conditions Agreement upon hire.	No exceptions noted.
CC1.1.1b		Inspected the signed agreements for a sample of new hires to confirm employees are required to acknowledge the Employee Terms and Conditions Agreement upon hire.	No exceptions noted.
CC1.1.2a	Employees are required to acknowledge the Employee Handbook as well as various policies and procedures that cover the Company's integrity and ethical values upon hire and annually thereafter.	Inquired with management to confirm employees are required to acknowledge the Employee Handbook as well as various policies and procedures that cover the Company's integrity and ethical values upon hire.	No exceptions noted.
CC1.1.2b		Inspected the acknowledgements for a sample of new hires to confirm employees are required to acknowledge the Employee Handbook as well as various policies and procedures that cover the Company's integrity and ethical values upon hire.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC1.1.2c		Inspected the Annual Employee Policy review for a sample of employees to confirm the annual acknowledgement of the Employee Handbook as well as various policies and procedures that cover the Company's integrity and ethical values.	No exceptions noted.
CC1.1.3	Employees who do not comply with Company policies and standards will be subject to disciplinary action.	Inspected company policies to confirm employees who do not comply with Company policies and standards will be subject to disciplinary action.	No exceptions noted.
CC1.1.4	Contractors with access to the environment are required to read and acknowledge Company policies and procedures related to information security.	Inspected the checklist for a sample of new contractors to confirm contractors with access to the environment are required to read and acknowledge Company policies and procedures related to information security.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1a	The Board of Directors meets monthly to review performance, initiatives, strategic direction, and finances. The Board is comprised of members independent from management.	Inspected the Governance Charter to confirm the Board of Directors meets monthly to review performance, initiatives, strategic direction, and finances.	No exceptions noted.
CC1.2.1b		Observed the Board of Directors meeting minutes for a sample of months to confirm the Board of Directors meets monthly to review performance, initiatives, strategic direction, and finances.	No exceptions noted.
CC1.2.1c		Inspected a listing of the members of the Board of Directors to confirm the Board is comprised of members independent from management.	No exceptions noted.
CC1.2.2a	The Leadership Team meets on a weekly basis to discuss operational action items, issues, etc. Additionally, the Team meets monthly to discuss strategic plans and updates.	Inspected the Governance Charter to confirm the Leadership Team meets on a weekly basis to discuss operational action items, issues, etc. and on a monthly basis to discuss strategic plans and updates.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC1.2.2b		Observed the Leadership Team meeting presentations for a sample of weeks to confirm the Leadership Team meets on a weekly basis to discuss operational action items, issues, etc.	Exception noted. The weekly Leadership Team Meeting did not occur in two (2) of the five (5) sampled weeks. See Section V below for management response.
CC1.2.2c		Observed the Leadership Team meeting presentations for a sample of months to confirm the Leadership Team meets monthly to discuss strategic plans and updates.	No exceptions noted.
CC1.2.3a	The Information Security Management Team (ISMS) is assigned the responsibility of implementing and overseeing the internal control environment. The team meets annually, with the Leadership Team, to discuss and review the internal control environment.	Inquired with management to confirm the Information Security Management team is assigned the responsibility of implementing and overseeing the internal control environment and meets annually with the Leadership Team to discuss and review the internal control environment.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC1.2.3b		Inspected the ISMS meeting minutes to confirm the Information Security Management team is assigned the responsibility of implementing and overseeing the internal control environment and meets annually with the Leadership Team to discuss and review the internal control environment.	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.			
CC1.3.1	The Company has documented an organizational chart that defines reporting lines.	Inspected the organizational chart to confirm the Company has documented an organizational chart that defines reporting lines.	No exceptions noted.
CC1.3.2a	The Company has documented job descriptions that define authorities and responsibilities. New descriptions will be developed prior to hiring for a position, if necessary.	Inquired with management to confirm new descriptions will be developed prior to hiring for a position, if necessary.	No exceptions noted.
CC1.3.2b		Inspected the job descriptions for a sample of employees to confirm the Company has documented job descriptions that define authorities and responsibilities.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC1.3.3a	The Board of Directors meets monthly to review performance, initiatives, strategic direction, and finances. The Board is comprised of members independent from management.	Inspected the Governance Charter to confirm the Board of Directors meets monthly to review performance, initiatives, strategic direction, and finances.	No exceptions noted.
CC1.3.3b		Observed the Board of Directors meeting minutes for a sample of months to confirm the Board of Directors meets monthly to review performance, initiatives, strategic direction, and finances.	No exceptions noted.
CC1.3.3c		Inspected a listing of the members of the Board of Directors to confirm the Board is comprised of members independent from management.	No exceptions noted.
CC1.3.4a	The Information Security Management Team (ISMS) is assigned the responsibility of implementing and overseeing the internal control environment. The team meets annually, with the Leadership Team, to discuss and review the internal control environment.	Inquired with management to confirm the Information Security Management team is assigned the responsibility of implementing and overseeing the internal control environment and meets annually with the Leadership Team to discuss and review the internal control environment.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC1.3.4b		Inspected the ISMS meeting minutes to confirm the Information Security Management team is assigned the responsibility of implementing and overseeing the internal control environment and meets annually with the Leadership Team to discuss and review the internal control environment.	No exceptions noted.
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1a	The Company performs checks on individual's background if the individual will have access to customer information upon hire and on an annual basis.	Inspected the background checks for a sample of new hires to confirm the Company performs checks on individual's background if the individual will have access to customer information.	No exceptions noted.
CC1.4.1b		Inspected the background checks for a sample of employees to confirm the Company performs checks on individual's background if the individual will have access to customer information on an annual basis.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC1.4.2	The Company performs several checks on prospective employees, including credit, education, and references.	Inspected the checks for a sample of new hires to confirm the Company performs several checks on prospective employees, including credit, education, and references.	Exception noted. One (1) of the three (3) sampled new hires did not have credit and reference checks prior to hire. See Section V below for management response.
CC1.4.3	The qualifications and skills of candidates are assessed by Human Resources and the hiring manager as part of the interview process.	Inquired with management to confirm the qualifications and skills of candidates are assessed by Human Resources and the hiring manager as part of the interview process.	No exceptions noted.
CC1.4.4a	Employees are required to complete security awareness training upon hire and annually thereafter.	Inspected the security awareness training completion for a sample of new hires to confirm employees are required to complete security awareness training upon hire.	No exceptions noted.
CC1.4.4b		Inspected the Annual Employee Policy review to confirm annual employee security awareness training was not completed during the audit period.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC1.4.5a	Employees undergo performance evaluations annually, which include a self-evaluation and manager review.	Inspected the Employee Handbook to confirm employees undergo performance evaluations annually, which include a self-evaluation and manager review.	No exceptions noted.
CC1.4.5b		Inspected the performance evaluations for employees to confirm employees did not undergo a performance evaluation during the audit period.	No exceptions noted.
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Employees who do not comply with Company policies and standards will be subject to disciplinary action.	Inspected company policies to confirm employees who do not comply with Company policies and standards will be subject to disciplinary action.	No exceptions noted.
CC1.5.2a	Employees undergo performance evaluations annually, which include a self-evaluation and manager review.	Inspected the Employee Handbook to confirm employees undergo performance evaluations annually, which include a self-evaluation and manager review.	No exceptions noted.
CC1.5.2b		Inspected the performance evaluations for employees to confirm employees did not undergo a performance evaluation during the audit period.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC2.0 - 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.			
CC2.1.1a	The Board of Directors meets monthly to review performance, initiatives, strategic direction, and finances. The Board is comprised of members independent from management.	Inspected the Governance Charter to confirm the Board of Directors meets monthly to review performance, initiatives, strategic direction, and finances.	No exceptions noted.
CC2.1.1b		Observed the Board of Directors meeting minutes for a sample of months to confirm the Board of Directors meets monthly to review performance, initiatives, strategic direction, and finances.	No exceptions noted.
CC2.1.1c		Inspected a listing of the members of the Board of Directors to confirm the Board is comprised of members independent from management.	No exceptions noted.
CC2.1.2a	The Leadership Team meets on a weekly basis to discuss operational action items, issues, etc. Additionally, the Team meets monthly to discuss strategic plans and updates.	Inspected the Governance Charter to confirm the Leadership Team meets on a weekly basis to discuss operational action items, issues, etc. and on a monthly basis to discuss strategic plans and updates.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC2.1.2b		Observed the Leadership Team meeting presentations for a sample of weeks to confirm the Leadership Team meets on a weekly basis to discuss operational action items, issues, etc.	Exception noted. The weekly Leadership Team Meeting did not occur in two (2) of the five (5) sampled weeks. See Section V below for management response.
CC2.1.2c		Observed the Leadership Team meeting presentations for a sample of months to confirm the Leadership Team meets monthly to discuss strategic plans and updates.	No exceptions noted.
CC2.1.3a	The Information Security Management Team (ISMS) is assigned the responsibility of implementing and overseeing the internal control environment. The team meets annually, with the Leadership Team, to discuss and review the internal control environment.	Inquired with management to confirm the Information Security Management team is assigned the responsibility of implementing and overseeing the internal control environment and meets annually with the Leadership Team to discuss and review the internal control environment.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC2.1.3b		Inspected the ISMS meeting minutes to confirm the Information Security Management team is assigned the responsibility of implementing and overseeing the internal control environment and meets annually with the Leadership Team to discuss and review the internal control environment.	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.			
CC2.2.1a	Employees are required to acknowledge the Employee Terms and Conditions Agreement upon hire.	Inquired with management to confirm employees are required to acknowledge the Employee Terms and Conditions Agreement upon hire.	No exceptions noted.
CC2.2.1b		Inspected the signed agreements for a sample of new hires to confirm employees are required to acknowledge the Employee Terms and Conditions Agreement upon hire.	No exceptions noted.
CC2.2.2a	Employees are required to complete security awareness training upon hire and annually thereafter.	Inspected the security awareness training completion for a sample of new hires to confirm employees are required to complete security awareness training upon hire.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC2.2.2b		Inspected the Annual Employee Policy review to confirm annual employee security awareness training was not completed during the audit period.	No exceptions noted.
CC2.2.3a	The Company has documented job descriptions that define authorities and responsibilities. New descriptions will be developed prior to hiring for a position, if necessary.	Inquired with management to confirm new descriptions will be developed prior to hiring for a position, if necessary.	No exceptions noted.
CC2.2.3b		Inspected the job descriptions for a sample of employees to confirm the Company has documented job descriptions that define authorities and responsibilities.	No exceptions noted.
CC2.2.4	Security reminders are sent, at least annually, to educate employees on security issues and recommended practices.	Inspected an example security reminder email to confirm security reminders are sent, at least annually, to educate employees on security issues and recommended practices.	No exceptions noted.
CC2.2.5a	A quarterly meeting is held with all employees to communicate strategic initiatives, operational changes and plan, internal controls, and performance metrics. Additionally, an annual Company Kickoff meeting is held with	Inspected meeting presentations for a sample of quarters to confirm a quarterly meeting is held with all employees to communicate strategic initiatives, operational changes and plan, internal controls, and performance metrics	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC2.2.5b	all employees to discuss the Company budget, hiring changes, and business objectives for the year.	Inspected a meeting presentation for the annual Company Kickoff meeting to confirm an annual Company Kickoff meeting is held with all employees to discuss the Company budget, hiring changes, and business objectives for the year.	No exceptions noted.
CC2.2.6	The Company's policies and procedures are made available to all employees via an internal site.	Inspected the internal site to confirm the Company's policies and procedures are made available to all employees via an internal site.	No exceptions noted.
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	All customers are required to sign a contract defining internal control responsibilities.	Inspected the contracts for a sample of new customers to confirm all customers are required to sign a contract defining internal control responsibilities.	No exceptions noted.
CC2.3.2a	Customers can submit issues and questions to the Company via their webpage. Issues will be tracked in a ticket and the customer can track the status of the issues through to remediation or see their support history.	Observed the Company's webpage to confirm customers can submit issues and questions.	No exceptions noted.
CC2.3.2b		Inspected the ticketing system to ensure all customer submitted issues and questions are tracked in a ticket and the customer can track the status of the issues through to remediation or see their support history.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC2.3.2c		Inspected the tickets for a sample of customer issues to confirm issues will be tracked in a ticket.	No exceptions noted.
CC2.3.3	Customer user group meetings are held annually to share upcoming product changes and updates. Customers have the opportunity to provide feedback.	Inspected the meeting presentation the customer user group meeting to confirm customer user group meetings are held annually to share upcoming product changes and updates and customers have the opportunity to provide feedback.	No exceptions noted.
CC2.3.4	Responsibilities of the Company and subservice organizations are documented in master service agreements.	Inspected the master service agreements for subservice organizations to confirm responsibilities of the Company and subservice organizations are documented in master service agreements.	No exceptions noted.
CC3.0 - 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.			
CC3.1.1	The Risk Management Process details the process for identifying potential threats, assessing the likelihood, and assessing the impact.	Inspected the Risk Management Process to confirm the Risk Management Process details the process for identifying potential threats, assessing the likelihood, and assessing the impact.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC3.1.2	The Supplier Management Policy defines expectations for identifying and risk rating all vendor relationships. The risk ratings consider the access to the Company's data and the criticality of the vendor to providing services.	Inspected the Supplier Management Policy to confirm the policy defines expectations for identifying and risk rating all vendor relationship and the risk ratings consider the access to the Company's data and the criticality of the vendor to providing services.	No exceptions noted.
CC3.1.3	The Risk Management Process defines criteria for risk mitigation and risk acceptance.	Inspected the Risk Management Process to confirm the policy defines criteria for risk mitigation and risk acceptance.	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.			
CC3.2.1	The Risk and Improvement Register addresses threat actors, the likelihood of an event, and the impact of an event.	Inspected the Risk Improvement Register to confirm it addresses threat actors, the likelihood of an event, and the impact of an event.	No exceptions noted.
CC3.2.2	The vendor risk assessment rates the risk of a vendor based on access to the Company data and the criticality of the vendor.	Inspected the vendor risk assessment to confirm the vendor risk assessment rates the risk of a vendor based on access to the Company data and the criticality of the vendor.	No exceptions noted.
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	The Risk and Improvement Register considers fraudulent activities, including the likelihood and impact.	Inspected the Risk and Improvement Register to confirm it considers fraudulent activities, including the likelihood and impact.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1a	The risk assessments are reviewed and approved annually by the Leadership Team.	Inspected the Risk and Improvement Register to confirm the risk assessment is reviewed and approved annually by the Leadership Team.	No exceptions noted.
CC3.4.1b		Inspected the Management Review meeting minutes to confirm the Risk and Improvement Register and the Vendor Risk Assessment are reviewed and approved annually by the Leadership Team.	No exceptions noted.
CC3.4.2	Policies and procedures are reviewed on an annual basis and updated, as needed.	Inspected the policy reviews to confirm the policies and procedures are reviewed on an annual basis and updated, as needed.	Exception noted. The Product Development Policy in effect for the audit period has not been formally approved since August 2021. See Section V below for management response.
CC3.4.3a	The Company subscribes to threat intelligence sources to identify changes and updates to the environment. Alerts received are reviewed and action is taken as necessary.	Inspected an example email to confirm the Company subscribes to threat intelligence sources to identify changes and updates to the environment.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC3.4.3b		Inquired to confirm alerts received are reviewed and action is taken as necessary.	No exceptions noted.
CC4.0 - 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.			
CC4.1.1a	Event log management solutions are configured to collect logs of user maintenance. Real-time alerts are generated and sent to appropriate personnel for specified user maintenance.	Inspected the configurations of the event log management solutions to confirm the event log management solutions are configured to collect logs of user maintenance.	No exceptions noted.
CC4.1.1b		Inspected the configurations of the event log management solutions to confirm real-time alerts are generated and sent to appropriate personnel for user maintenance.	No exceptions noted.
CC4.1.1c		Inspected example alerts to confirm real-time alerts are generated and sent to appropriate personnel for user maintenance.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC4.1.2a	Solutions are configured to collect logs of performance and capacity metrics. The solutions are configured to monitor capacity and availability metrics for the system including disk usage, memory usage, processor load, and server downtime/ uptime. An alert is generated to appropriate personnel when defined performance metrics are exceeded.	Inspected the configurations of the solutions to confirm the solutions are configured to collect log and to monitor capacity and availability metrics for the system including disk usage, memory usage, processor load, and server downtime/uptime.	No exceptions noted.
CC4.1.2b		Inspected the configurations of the solutions to confirm appropriate individuals are alerted when defined performance metrics are exceeded.	No exceptions noted.
CC4.1.2c		Inspected example alerts to confirm alerts are generated to appropriate personnel when defined performance metrics are exceeded.	No exceptions noted.
CC4.1.3a	A solution is configured to monitor the production environment and an alert is generated to appropriate personnel when the production environment is down.	Inspected the solution configurations to confirm a solution is configured to monitor the production environment and an alert is generated to appropriate personnel when the production environment is down.	No exceptions noted.
CC4.1.3b		Inspected an example alert to confirm a solution is configured to monitor the production environment and an alert is generated to appropriate personnel when the production environment is down.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC4.1.4a	Internal vulnerability scans are run continuously on the infrastructure software. On an at least quarterly basis management reviews the results to ensure the software is patched appropriately. All vulnerabilities are assigned a vulnerability rating that dictates the timeframe for remediation.	Inspected the Vulnerability Management Policy to confirm vulnerability scans are run continuously on the infrastructure software and on an at least quarterly basis management reviews the results to ensure the software is patched appropriately. All vulnerabilities are assigned a vulnerability rating that dictates the timeframe for remediation.	No exceptions noted.
CC4.1.4b		Inspected vulnerability scan configurations to confirm vulnerability scans are run continuously on the infrastructure software.	No exceptions noted.
CC4.1.4c		Observed example tickets to confirm vulnerability scans are run continuously on the infrastructure software and on an at least quarterly basis management reviews the results to ensure the software is patched appropriately.	No exceptions noted.
CC4.1.5a	A third-party is contracted to perform penetration testing against the production environment on an annual basis. All results are reviewed by management and remediation action(s) plans are created and tracked through remediation.	Inspected the penetration testing report to confirm there was an annual penetration test completed against the production environment.	No exceptions noted.
CC4.1.5b		Inquired with management to confirm all results are reviewed by management and remediation action(s) plans are created and tracked through remediation.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC4.1.6	User access for the technologies supporting the system is reviewed for appropriateness on a semi-annual basis.	Inspected the user access reviews performed to confirm user access for the technologies supporting the system is reviewed for appropriateness on a semi-annual basis.	No exceptions noted.
CC4.1.7	Controls relating to the monitoring, evaluating, communicating, and correcting of cloud infrastructure security, performance, and events are the responsibility of the subservice organizations AWS and Microsoft. See the Complementary Subservice Organization Controls above for additional details.		
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.			
CC4.2.1a	Event log management solutions are configured to collect logs of user maintenance. Real-time alerts are generated and sent to appropriate personnel for specified user maintenance.	Inspected the configurations of the event log management solutions to confirm the event log management solutions are configured to collect logs of user maintenance.	No exceptions noted.
CC4.2.1b		Inspected the configurations of the event log management solutions to confirm real-time alerts are generated and sent to appropriate personnel for user maintenance.	No exceptions noted.
CC4.2.1c		Inspected example alerts to confirm real-time alerts are generated and sent to appropriate personnel for user maintenance.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC4.2.2a	Solutions are configured to collect logs of performance and capacity metrics. The solutions are configured to monitor capacity and availability metrics for the system including disk usage, memory usage, processor load, and server downtime/uptime. An alert is generated to appropriate personnel when defined performance metrics are exceeded.	Inspected the configurations of the solutions to confirm the solutions are configured to collect log and to monitor capacity and availability metrics for the system including disk usage, memory usage, processor load, and server downtime/uptime.	No exceptions noted.
CC4.2.2b		Inspected the configurations of the solutions to confirm appropriate individuals are alerted when defined performance metrics are exceeded.	No exceptions noted.
CC4.2.2c		Inspected example alerts to confirm alerts are generated to appropriate personnel when defined performance metrics are exceeded.	No exceptions noted.
CC4.2.3a	A solution is configured to monitor the production environment and an alert is generated to appropriate personnel when the production environment is down.	Inspected the solution configurations to confirm a solution is configured to monitor the production environment and an alert is generated to appropriate personnel when the production environment is down.	No exceptions noted.
CC4.2.3b		Inspected an example alert to confirm a solution is configured to monitor the production environment and an alert is generated to appropriate personnel when the production environment is down.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC4.2.4a	Internal vulnerability scans are run continuously on the infrastructure software. On an at least quarterly basis management reviews the results to ensure the software is patched appropriately. All vulnerabilities are assigned a vulnerability rating that dictates the timeframe for remediation.	Inspected the Vulnerability Management Policy to confirm vulnerability scans are run continuously on the infrastructure software and on an at least quarterly basis management reviews the results to ensure the software is patched appropriately. All vulnerabilities are assigned a vulnerability rating that dictates the timeframe for remediation.	No exceptions noted.
CC4.2.4b		Inspected vulnerability scan configurations to confirm vulnerability scans are run continuously on the infrastructure software.	No exceptions noted.
CC4.2.4c		Observed example tickets to confirm vulnerability scans are run continuously on the infrastructure software and on an at least quarterly basis management reviews the results to ensure the software is patched appropriately.	No exceptions noted.
CC4.2.5a	A third-party is contracted to perform penetration testing against the production environment on an annual basis. All results are reviewed by management and remediation action(s) plans are created and tracked through remediation.	Inspected the penetration testing report to confirm there was an annual penetration test completed against the production environment.	No exceptions noted.
CC4.2.5b		Inquired with management to confirm all results are reviewed by management and remediation action(s) plans are created and tracked through remediation.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC4.2.6a	The Leadership Team meets on a weekly basis to discuss operational action items, issues, etc. Additionally, the Team meets monthly to discuss strategic plans and updates.	Inspected the Governance Charter to confirm the Leadership Team meets on a weekly basis to discuss operational action items, issues, etc. and on a monthly basis to discuss strategic plans and updates.	No exceptions noted.
CC4.2.6b		Observed the Leadership Team meeting presentations for a sample of weeks to confirm the Leadership Team meets on a weekly basis to discuss operational action items, issues, etc.	Exception noted. The weekly Leadership Team Meeting did not occur in two (2) of the five (5) sampled weeks. See Section V below for management response.
CC4.2.6c		Observed the Leadership Team meeting presentations for a sample of months to confirm the Leadership Team meets monthly to discuss strategic plans and updates.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC5.0 - 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.			
CC5.1.1	The Risk and Improvement Register details appropriate controls to lessen the likelihood and/or impact of identified risks.	Inspected the Risk and Improvement Register to confirm it details appropriate controls to lessen the likelihood and/or impact of identified risks.	No exceptions noted.
CC5.1.2	The Risk Management Process details a methodology for the Company to identify and apply appropriate controls to lessen the likelihood and/or impact of identified risks.	Inspected the Risk Management Process to confirm the policy details a methodology for the Company to identify and apply appropriate controls to lessen the likelihood and/or impact of identified risks.	No exceptions noted.
CC5.1.3	The Risk Management Process defines criteria for risk mitigation and risk acceptance.	Inspected the Risk Management Process to confirm the policy defines criteria for risk mitigation and risk acceptance.	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.			
CC5.2.1a	Event log management solutions are configured to collect logs of user maintenance. Real-time alerts are generated and sent to appropriate personnel for specified user maintenance.	Inspected the configurations of the event log management solutions to confirm the event log management solutions are configured to collect logs of user maintenance.	No exceptions noted.
CC5.2.1b		Inspected the configurations of the event log management solutions to confirm real-time alerts are generated and sent to appropriate personnel for user maintenance.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC5.2.1c		Inspected example alerts to confirm real-time alerts are generated and sent to appropriate personnel for user maintenance.	No exceptions noted.
CC5.2.2a	Internal vulnerability scans are run continuously on the infrastructure software. On an at least quarterly basis, management reviews the results to ensure the software is patched appropriately. All vulnerabilities are assigned a vulnerability rating that dictates the timeframe for remediation.	Inspected the Vulnerability Management Policy to confirm vulnerability scans are run continuously on the infrastructure software and on an at least quarterly basis management reviews the results to ensure the software is patched appropriately. All vulnerabilities are assigned a vulnerability rating that dictates the timeframe for remediation.	No exceptions noted.
CC5.2.2b		Inspected vulnerability scan configurations to confirm vulnerability scans are run continuously on the infrastructure software.	No exceptions noted.
CC5.2.2c		Observed example tickets to confirm vulnerability scans are run continuously on the infrastructure software and on an at least quarterly basis management reviews the results to ensure the software is patched appropriately.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC5.2.3a	A third-party is contracted to perform penetration testing against the production environment on an annual basis. All results are reviewed by management and remediation action(s) plans are created and tracked through remediation.	Inspected the penetration testing report to confirm there was an annual penetration test completed against the production environment.	No exceptions noted.
CC5.2.3b		Inquired with management to confirm all results are reviewed by management and remediation action(s) plans are created and tracked through remediation.	No exceptions noted.
CC5.2.4	An independent party is contracted to perform an ISO certifications on an annual basis.	Inspected the ISO certifications report to confirm an independent party is contracted to perform ISO certifications on an annual basis.	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.			
CC5.3.1	Control activities are defined in policies and procedures.	Inspected the Company's policies and procedures to confirm control activities are defined in policies and procedures.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC5.3.2	Policies and procedures are reviewed on an annual basis and updated, as needed.	Inspected the policy reviews to confirm the policies and procedures are reviewed on an annual basis and updated, as needed.	Exception noted. The Product Development Policy in effect for the audit period has not been formally approved since August 2021. See Section V below for management response.
CC6.0 - 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.			
CC6.1.1a	Logical access to technologies supporting the system is restricted to appropriate personnel who require access to perform their job functions. Unique IDs are assigned for access.	Inspected the user listings for the Azure Server to confirm logical access is restricted to appropriate personnel who require access to perform their job functions and unique IDs are assigned for access.	No exceptions noted.
CC6.1.1b		Inspected the user listings for the Azure Console to confirm logical access is restricted to appropriate personnel who require access to perform their job functions and unique IDs are assigned for access.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC6.1.1c		Inspected the user listings for AWS to confirm logical access is restricted to appropriate personnel who require access to perform their job functions and unique IDs are assigned for access.	No exceptions noted.
CC6.1.1d		Inspected the user listings for the MySQL Database to confirm logical access is restricted to appropriate personnel who require access to perform their job functions and unique IDs are assigned for access.	No exceptions noted.
CC6.1.1e		Inspected the user listings for the Secure File Transfer Protocol (SFTP) Server to confirm logical access is restricted to appropriate personnel who require access to perform their job functions and unique IDs are assigned for access.	No exceptions noted.
CC6.1.2a	Administrator level access to technologies supporting the system is restricted to appropriate personnel who require the access to oversee the system.	Inspected the user listings for the Azure Server to confirm administrator level access is restricted to appropriate personnel who require the access to oversee the system.	No exceptions noted.
CC6.1.2b		Inspected the user listings for the Azure Console to confirm administrator level access is restricted to appropriate personnel who require the access to oversee the system.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC6.1.2c		Inspected the user listings for AWS to confirm administrator level access is restricted to appropriate personnel who require the access to oversee the system.	No exceptions noted.
CC6.1.2d		Inspected the user listings for the MySQL Database to confirm administrator level access is restricted to appropriate personnel who require the access to oversee the system.	No exceptions noted.
CC6.1.2e		Inspected the user listings for the SFTP Server to confirm administrator level access is restricted to appropriate personnel who require the access to oversee the system.	No exceptions noted.
CC6.1.3a	Multifactor authentication is used to access the technologies supporting the system, where possible.	Observed the authentication requirements for the Azure Server to confirm multifactor authentication is enforced.	No exceptions noted.
CC6.1.3b		Observed the authentication requirements for the Azure Console to confirm multifactor authentication is enforced.	No exceptions noted.
CC6.1.3c		Inspected the authentication requirements for AWS to confirm multifactor authentication is enforced.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC6.1.3d		Observed the authentication requirements for the MySQL Database to confirm multifactor authentication is enforced.	No exceptions noted.
CC6.1.4	The SFTP site enforces a strong password.	Inspected the SFTP password requirements to confirm the SFTP site enforces a strong password.	No exceptions noted.
CC6.1.5	Customer data is logically separated so customers can only see their own information.	Inspected the environment configurations to confirm customer data is logically separated so customers can only see their own information.	No exceptions noted.
CC6.1.6a	Users are authenticated to the system through a userID and password. The connection to the system is encrypted.	Inspected the login page to confirm users are authenticated to the system through a userID and password.	No exceptions noted.
CC6.1.6b		Inspected the encryption certificate for Preservica to confirm the connection is encrypted.	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.			
CC6.2.1a	Written authorization is required from the Line Manager to the IT department to request system access for all new hires. A User Access Control spreadsheet is maintained detailing the specific access for the individual.	Inspected the Access Control Procedure to confirm written authorization is required from the Line Manager to the IT department to request system access for all new hires and a User Access Control spreadsheet is maintained detailing the specific access for the individual.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC6.2.1b		Inspected onboarding tickets for a sample of new hires to confirm written authorization is required from the Line Manager to the IT department to request system access for all new hires and a User Access Control spreadsheet is maintained detailing the specific access for the individual.	No exceptions noted.
CC6.2.2a	Written authorization is required from the Line Manager to the IT department to request system removal for all terminations. A User Access Control spreadsheet is maintained detailing the specific access removal for the individual.	Inspected the Access Control Procedure to confirm written authorization is required from the Line Manager to the IT department to request system removal for all terminations and a User Access Control spreadsheet is maintained detailing the specific access removal for the individual.	No exceptions noted.
CC6.2.2b		Inspected the IT Leaver Checklist for a sample of terminations to confirm written authorization is required from the Line Manager to the IT department to request system removal for all terminations and a User Access Control spreadsheet is maintained detailing the specific access removal for the individual.	No exceptions noted.
CC6.2.3	Written authorization is required to setup and remove customer access to the SFTP server.	Inspected the tickets for a sample of new customers to confirm written authorization is required to setup customer access to the SFTP server.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC6.2.4a	Written authorization is required to setup customer administrator access to the system.	Inquired with management to confirm written authorization is required to setup customer administrator access to the system.	No exceptions noted.
CC6.2.4b		Inspected tickets for a sample of new customers to confirm written authorization is required to setup customer administrator access to the system.	No exceptions noted.
CC6.2.5a	Written authorization is required is required to request granting system access for all new consultants and removal for all terminated consultants.	Inspected the written authorization for a sample of new consultants to confirm written authorization is required to request granting system access for all new consultants.	No exceptions noted.
CC6.2.5b		Inspected the written authorization for a sample of terminated consultants to confirm written authorization is required to request system removal for all terminated consultants.	Exception noted. One (1) of the three (3) sampled terminated consultant did not have access revoked in a timely manner. See Section V below for management response.

Key	Service Organization Controls	Tests	Results
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.			
CC6.3.1a	Written authorization is required from the Line Manager to the IT department to request system access for all new hires. A User Access Control spreadsheet is maintained detailing the specific access for the individual.	Inspected the Access Control Procedure to confirm written authorization is required from the Line Manager to the IT department to request system access for all new hires and a User Access Control spreadsheet is maintained detailing the specific access for the individual.	No exceptions noted.
CC6.3.1b		Inspected onboarding tickets for a sample of new hires to confirm written authorization is required from the Line Manager to the IT department to request system access for all new hires and a User Access Control spreadsheet is maintained detailing the specific access for the individual.	No exceptions noted.
CC6.3.2a	Written authorization is required from the Line Manager to the IT department to request system removal for all terminations. A User Access Control spreadsheet is maintained detailing the specific access removal for the individual.	Inspected the Access Control Procedure to confirm written authorization is required from the Line Manager to the IT department to request system removal for all terminations and a User Access Control spreadsheet is maintained detailing the specific access removal for the individual.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC6.3.2b		Inspected the IT Leaver Checklist for a sample of terminations to confirm written authorization is required from the Line Manager to the IT department to request system removal for all terminations and a User Access Control spreadsheet is maintained detailing the specific access removal for the individual.	No exceptions noted.
CC6.3.3	Written authorization is required to setup and remove customer access to the SFTP server.	Inspected the tickets for a sample of new customers to confirm written authorization is required to setup customer access to the SFTP server.	No exceptions noted.
CC6.3.4a	Written authorization is required to setup customer administrator access to the system.	Inquired with management to confirm written authorization is required to setup customer administrator access to the system.	No exceptions noted.
CC6.3.4b		Inspected tickets for a sample of new customers to confirm written authorization is required to setup customer administrator access to the system.	No exceptions noted.
CC6.3.5a	Written authorization is required is required to request granting system access for all new consultants and removal for all terminated consultants.	Inspected the written authorization for a sample of new consultants to confirm written authorization is required to request granting system access for all new consultants.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC6.3.5b		Inspected the written authorization for a sample of terminated consultants to confirm written authorization is required to request system removal for all terminated consultants.	Exception noted. One (1) of the three (3) sampled terminated consultant did not have access revoked in a timely manner. See Section V below for management response.
CC6.3.6	User access for the technologies supporting the system is reviewed for appropriateness on a semi-annual basis.	Inspected the user access reviews performed to confirm user access for the technologies supporting the system is reviewed for appropriateness on a semi-annual basis.	No exceptions noted.
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.			
CC6.4.1	Controls relating to physical security to restrict access to their data centers, facilities, and protected information assets to authorized personnel are administered by the subservice organizations AWS and Microsoft. See the Complementary Subservice Organization Controls above for additional details.		
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.			
CC6.5.1	Controls relating to the destruction and disposal of hardware administered are the responsibility of the subservice organizations AWS and Microsoft. See the Complementary Subservice Organization Controls above for additional details.		

Key	Service Organization Controls	Tests	Results
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1a	Internal vulnerability scans are run continuously on the infrastructure software. On an at least quarterly basis management reviews the results to ensure the software is patched appropriately. All vulnerabilities are assigned a vulnerability rating that dictates the timeframe for remediation.	Inspected the Vulnerability Management Policy to confirm vulnerability scans are run continuously on the infrastructure software and on an at least quarterly basis management reviews the results to ensure the software is patched appropriately. All vulnerabilities are assigned a vulnerability rating that dictates the timeframe for remediation.	No exceptions noted.
CC6.6.1b		Inspected vulnerability scan configurations to confirm vulnerability scans are run continuously on the infrastructure software.	No exceptions noted.
CC6.6.1c		Observed example tickets to confirm vulnerability scans are run continuously on the infrastructure software and on an at least quarterly basis management reviews the results to ensure the software is patched appropriately.	No exceptions noted.
CC6.6.2a	A third-party is contracted to perform penetration testing against the production environment on an annual basis. All results are reviewed by management and remediation action(s) plans are created and tracked through remediation.	Inspected the penetration testing report to confirm there was an annual penetration test completed against the production environment.	No exceptions noted.
CC6.6.2b		Inquired with management to confirm all results are reviewed by management and remediation action(s) plans are created and tracked through remediation.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC6.6.3a	External access by employees to the network is permitted only through an encrypted VPN connection. Authentication requires employees to enter their network credentials followed by a one-time code.	Inspected the VPN authentication requirements to confirm external access by employees to the network is permitted only through an encrypted VPN connection and authentication requires employees to enter their network credentials followed by a one-time code.	No exceptions noted.
CC6.6.3b		Inspected the user listing for the VPN to confirm logical access to the VPN is restricted to appropriate personnel who require access to perform their job functions.	No exceptions noted.
CC6.6.4a	All users are required to authenticate to the SFTP Server via username and password. Communications with the SFTP server are encrypted.	Observed the SFTP Server authentication to confirm all users are required to authenticate to the SFTP Server via username and password.	No exceptions noted.
CC6.6.4b		Inspected the SFTP Server encryption to confirm communications with the SFTP server are encrypted.	No exceptions noted.
CC6.6.5a	Users are authenticated to the system through a userID and password. The connection to the system is encrypted.	Inspected the login page to confirm users are authenticated to the system through a userID and password.	No exceptions noted.
CC6.6.5b		Inspected the encryption certificate for Preservica to confirm the connection is encrypted.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
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.			
CC6.7.1a	External access by employees to the network is permitted only through an encrypted VPN connection. Authentication requires employees to enter their network credentials followed by a one-time code.	Inspected the VPN authentication requirements to confirm external access by employees to the network is permitted only through an encrypted VPN connection and authentication requires employees to enter their network credentials followed by a one-time code.	No exceptions noted.
CC6.7.1b		Inspected the user listing for the VPN to confirm logical access to the VPN is restricted to appropriate personnel who require access to perform their job functions.	No exceptions noted.
CC6.7.2a	All users are required to authenticate to the SFTP Server via username and password. Communications with the SFTP server are encrypted.	Observed the SFTP Server authentication to confirm all users are required to authenticate to the SFTP Server via username and password.	No exceptions noted.
CC6.7.2b		Inspected the SFTP Server encryption to confirm communications with the SFTP server are encrypted.	No exceptions noted.
CC6.7.3	Backup data is encrypted at rest and in transit.	Inspected the backup configurations to confirm backup data is encrypted at rest and in transit.	No exceptions noted.
CC6.7.4a	Users are authenticated to the system through a userID and password. The connection to the system is encrypted.	Inspected the login page to confirm users are authenticated to the system through a userID and password.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC6.7.4b		Inspected the encryption certificate for Preservica to confirm the connection is encrypted.	No exceptions noted.
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.			
CC6.8.1	The ability to promote application code changes into the production environment is restricted to the Operations team.	Inquired with management to confirm the ability to promote application code changes into the production environment is limited to the Operations team.	No exceptions noted.
CC6.8.2a	Internal vulnerability scans are run continuously on the infrastructure software. On an at least quarterly basis management reviews the results to ensure the software is patched appropriately. All vulnerabilities are assigned a vulnerability rating that dictates the timeframe for remediation.	Inspected the Vulnerability Management Policy to confirm vulnerability scans are run continuously on the infrastructure software and on an at least quarterly basis management reviews the results to ensure the software is patched appropriately. All vulnerabilities are assigned a vulnerability rating that dictates the timeframe for remediation.	No exceptions noted.
CC6.8.2b		Inspected vulnerability scan configurations to confirm vulnerability scans are run continuously on the infrastructure software.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC6.8.2c		Observed example tickets to confirm vulnerability scans are run continuously on the infrastructure software and on an at least quarterly basis management reviews the results to ensure the software is patched appropriately.	No exceptions noted.
CC6.8.3a	A third-party is contracted to perform penetration testing against the production environment on an annual basis. All results are reviewed by management and remediation action(s) plans are created and tracked through remediation.	Inspected the penetration testing report to confirm there was an annual penetration test completed against the production environment.	No exceptions noted.
CC6.8.3b		Inquired with management to confirm all results are reviewed by management and remediation action(s) plans are created and tracked through remediation.	No exceptions noted.
CC6.8.4a	Critical and security patches are applied to servers during the release cycle.	Inspected the Patch Management Policy to confirm critical and security patches are applied to servers during the release cycle.	No exceptions noted.
CC6.8.4b		Inspected the patching reports for a sample of releases to confirm critical and security patches are applied to servers during the release cycle.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC7.0 - 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.			
CC7.1.1a	Internal vulnerability scans are run continuously on the infrastructure software. On an at least quarterly basis management reviews the results to ensure the software is patched appropriately. All vulnerabilities are assigned a vulnerability rating that dictates the timeframe for remediation.	Inspected the Vulnerability Management Policy to confirm vulnerability scans are run continuously on the infrastructure software and on an at least quarterly basis management reviews the results to ensure the software is patched appropriately. All vulnerabilities are assigned a vulnerability rating that dictates the timeframe for remediation.	No exceptions noted.
CC7.1.1b		Inspected vulnerability scan configurations to confirm vulnerability scans are run continuously on the infrastructure software.	No exceptions noted.
CC7.1.1c		Observed example tickets to confirm vulnerability scans are run continuously on the infrastructure software and on an at least quarterly basis management reviews the results to ensure the software is patched appropriately.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC7.1.2a	A third-party is contracted to perform penetration testing against the production environment on an annual basis. All results are reviewed by management and remediation action(s) plans are created and tracked through remediation.	Inspected the penetration testing report to confirm there was an annual penetration test completed against the production environment.	No exceptions noted.
CC7.1.2b		Inquired with management to confirm all results are reviewed by management and remediation action(s) plans are created and tracked through remediation.	No exceptions noted.
CC7.1.3a	Event log management solutions are configured to collect logs of user maintenance. Real-time alerts are generated and sent to appropriate personnel for specified user maintenance.	Inspected the configurations of the event log management solutions to confirm the event log management solutions are configured to collect logs of user maintenance.	No exceptions noted.
CC7.1.3b		Inspected the configurations of the event log management solutions to confirm real-time alerts are generated and sent to appropriate personnel for user maintenance.	No exceptions noted.
CC7.1.3c		Inspected example alerts to confirm real-time alerts are generated and sent to appropriate personnel for user maintenance.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
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.			
CC7.2.1a	Solutions are configured to collect logs of performance and capacity metrics. The solutions are configured to monitor capacity and availability metrics for the system including disk usage, memory usage, processor load, and server downtime/uptime. An alert is generated to appropriate personnel when defined performance metrics are exceeded.	Inspected the configurations of the solutions to confirm the solutions are configured to collect log and to monitor capacity and availability metrics for the system including disk usage, memory usage, processor load, and server downtime/uptime.	No exceptions noted.
CC7.2.1b		Inspected the configurations of the solutions to confirm appropriate individuals are alerted when defined performance metrics are exceeded.	No exceptions noted.
CC7.2.1c		Inspected example alerts to confirm alerts are generated to appropriate personnel when defined performance metrics are exceeded.	No exceptions noted.
CC7.2.2a	A solution is configured to monitor the production environment and an alert is generated to appropriate personnel when the production environment is down.	Inspected the solution configurations to confirm a solution is configured to monitor the production environment and an alert is generated to appropriate personnel when the production environment is down.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC7.2.2b		Inspected an example alert to confirm a solution is configured to monitor the production environment and an alert is generated to appropriate personnel when the production environment is down.	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.			
CC7.3.1	The Incident Management Procedure details procedures for identifying, assessing, containing, mitigating, and recovering from incidents.	Inspected the Incident Management Procedure to confirm the policy details procedures for identifying, assessing, containing, mitigating, and recovering from incidents.	No exceptions noted.
CC7.3.2	Employees will communicate potential incidents to designated personnel so appropriate actions may be taken.	Inspected the Incident Management Procedures to confirm employees will communicate potential incidents to designated personnel so appropriate actions may be taken.	No exceptions noted.
CC7.3.3a	Incidents are assessed to evaluate the exposure/impact of an incident. All incidents are tracked in an incident log.	Inspected the Incident Management Procedure to confirm incidents are assessed to evaluate the exposure/impact of an incident and tracked in an incident log.	No exceptions noted.
CC7.3.3b		Inspected the logs for a sample of incidents to confirm incidents are assessed to evaluate the exposure/impact of an incident and tracked in an incident log.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
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.			
CC7.4.1	The Incident Management Procedure defines steps for communicating externally applicable parties, when necessary, including, regulators, law enforcement, and/or customers.	Inspected the Incident Management Procedure to confirm the policy defines steps for communicating externally applicable parties, when necessary, including, regulators, law enforcement, and/or customers.	No exceptions noted.
CC7.4.2	The Incident Management Procedure details procedures for identifying, assessing, containing, mitigating, and recovering from incidents.	Inspected the Incident Management Procedure to confirm the policy details procedures for identifying, assessing, containing, mitigating, and recovering from incidents.	No exceptions noted.
CC7.4.3	Employees will communicate potential incidents to designated personnel so appropriate actions may be taken.	Inspected the Incident Management Procedures to confirm employees will communicate potential incidents to designated personnel so appropriate actions may be taken.	No exceptions noted.
CC7.4.4a	Employees are required to acknowledge the Incident Management Procedure upon hire and annually thereafter.	Inquired with management to confirm employees are required to acknowledge the Incident Management Procedure upon hire and annually thereafter.	No exceptions noted.
CC7.4.4b		Inspected the acknowledgements for a sample of new hires to confirm employees are required to acknowledge the Incident Management Procedure upon hire.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC7.4.4c		Inspected the Annual Employee Policy review to confirm the annual acknowledgement of the Incident Management Procedure were completed during the audit period.	No exceptions noted.
CC7.4.5a	The Leadership team does an analysis of incidents occurred during the annual Information Security Management Team (ISMS) meeting. If the analysis indicates a weakness in the control environment, additional controls will be discussed and introduced within the Risk Register.	Inspected the Incident Management Procedure to confirm the Leadership team does an analysis of incidents occurred during the annual ISMS meeting.	No exceptions noted.
CC7.4.5b		Inspected the ISMS meeting minutes to confirm the Leadership team does an analysis of incidents occurred during the annual ISMS meeting and if the analysis indicates a weakness in the control environment, additional controls will be discussed and introduced within the Risk Register.	No exceptions noted.
CC7.4.6	Controls related to monitoring the environment to maintain security and availability including having an incident handling process, are the responsibility of the subservice organizations AWS and Microsoft. See the Complementary Subservice Organization Controls above for additional details.		
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The Incident Management Procedure details procedures for identifying, assessing, containing, mitigating, and recovering from incidents.	Inspected the Incident Management Procedure to confirm the policy details procedures for identifying, assessing, containing, mitigating, and recovering from incidents.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC7.5.2	The Company has purchased insurance policies to offset the financial impact of business disruptions, including disruptions arising from cyber events.	Inspected the insurance policy to confirm the Company has purchased insurance policies to offset the financial impact of business disruptions, including disruptions arising from cyber events.	No exceptions noted.
CC7.5.3a	All production data is backed up on at least a daily basis. All backups are encrypted while in transit and at rest. All backup data is retained for at least thirty (30) days.	Inspected the Backup and Restore Policy to confirm all production data is backed up on at least a daily basis and retained for thirty (30) days.	No exceptions noted.
CC7.5.3b		Inspected the backup configurations to confirm all production data is backed up on at least a daily basis, retained for thirty (30) days, and is encrypted while in transit and at rest.	No exceptions noted.
CC7.5.4a	Appropriate personnel are notified of failures or errors during the backup process for investigation.	Inspected the backup configurations to confirm appropriate personnel are notified of failures or errors during the backup process for investigation.	No exceptions noted.
CC7.5.4b		Inquired with management to confirm there were no AWS backup failures to verify appropriate personnel are notified during the audit period. Therefore, the Service Auditor was unable to test the operating effectiveness of the control during the audit period.	Control did not operate during the period.

Key	Service Organization Controls	Tests	Results
CC7.5.4c		Inspected an example Azure alert to confirm appropriate personnel are notified of failures or errors during the backup process for investigation.	No exceptions noted.
CC7.5.5a	Backup restore tests are performed on a semi-annual basis to validate the integrity of data backups.	Inspected the Backup Procedure to confirm backup restore tests are performed on a semi-annual basis to validate the integrity of data backups.	No exceptions noted.
CC7.5.5b		Inspected the most recent backup restore tests to confirm backup restore tests are performed on a semi-annual basis to validate the integrity of data backups.	No exceptions noted.
CC8.0 - Change Management			
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	The Company has defined a product development process that addresses business requirements, design, testing, acceptance, and implementation.	Inspected the Product Development Policy to confirm the Company has defined a product development process that addresses business requirements, design, testing, acceptance, and implementation.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC8.1.2a	Product developments are documented in tickets and undergo quality assurance prior to implementation. The tickets include a description of the development as well as quality assurance testing.	Inspected the Product Development Policy to confirm the product developments are documented in tickets and undergo quality assurance prior to implementation.	No exceptions noted.
CC8.1.2b		Inspected the tickets for a sample of developments to confirm the product developments are documented in tickets that include a description of the development as well as quality assurance testing.	No exceptions noted.
CC8.1.3a	Squads hold daily standup meetings to discuss the progress on new developments and the plan for the day.	Inquired with management to confirm the squads hold daily standup meetings to discuss the progress on new developments and the plan for the day.	No exceptions noted.
CC8.1.3b		Inspected the meeting invites for a sample of days to confirm the squads hold daily standup meetings to discuss the progress on new developments and the plan for the day.	No exceptions noted.
CC8.1.4	Product releases that impact customers are communicated via email updates and/or the customer portal.	Inspected communications for a sample of product releases to confirm product releases that impact customers are communicated via email updates and/or the customer portal.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC8.1.5	The Change Management Procedure addresses the process for authorization, testing, and approval of system changes.	Inspected the Change Management Process to confirm the Change Management Procedure addresses the process for authorization, testing, and approval of system changes.	No exceptions noted.
CC8.1.6a	All standard change requests are formally documented and detail a description of the changes.	Inspected the Change Management Process to confirm standard change requests are formally documented and detail a description of the changes.	No exceptions noted.
CC8.1.6b		Inspected the change requests for a sample of standard changes to confirm change requests are formally documented and detail a description of the changes.	No exceptions noted.
CC8.1.7a	All normal change requests are formally documented and detail a description of the changes as well as the review/approval.	Inspected the Change Management Process to confirm normal change requests are formally documented and detail a description of the changes as well as the approval.	No exceptions noted.
CC8.1.7b		Inspected the change requests for a sample of normal changes to confirm change requests are formally documented and detail a description of the changes as well as the review/approval.	No exceptions noted.
CC8.1.8a	Emergency change requests are verbally approved and will be documented after the fact.	Inspected the Change Management Process to confirm emergency change requests are verbally approved and will be documented after the fact.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC8.1.8b		Inquired with management to confirm there were no emergency changes in the audit period. Therefore, the Service Auditor was unable to test the operating effectiveness of the control during the audit period.	Control did not operate during the period.
CC8.1.9a	Bi-weekly meetings are held by the Cloud Ops team to review the recently performed changes and upcoming changes.	Inquired with management to confirm bi-weekly meetings are held by the Cloud Ops team to review the recently performed changes and upcoming changes.	No exceptions noted.
CC8.1.9b		Inspected the meeting minutes for a sample of bi-weekly meetings to confirm bi-weekly meetings are held by the Cloud Ops team to review the recently performed changes and upcoming changes.	No exceptions noted.
CC8.1.10	Controls related to changing the infrastructure supporting the environment are the responsibility of the subservice organizations AWS and Microsoft. See the Complementary Subservice Organization Controls above for additional details.		

Key	Service Organization Controls	Tests	Results
CC9.0 - Risk Mitigation			
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	The Business Continuity Plan and Disaster Recovery Procedures addresses recovering connectivity and supporting systems to ensure customer obligations can be met.	Inspected Business Continuity Plan and Disaster Recovery Procedures to confirm the policies and procedures address recovering connectivity and supporting systems to ensure customer obligations can be met.	No exceptions noted.
CC9.1.2a	The Business Continuity Plan is tested by the Company on an annual basis and the Disaster Recovery Procedures are to be tested on a semi-annual basis.	Inspected the Business Continuity Plan and Disaster Recovery Procedures to confirm the Business Continuity Plan is tested by the Company on an annual basis and the Disaster Recovery Procedures are to be tested on a quarterly basis.	No exceptions noted.
CC9.1.2b		Inspected the annual Business Continuity Plan test results to confirm the Business Continuity Plan was not tested during the audit period.	No exceptions noted.
CC9.1.2c		Inspected the testing for the Disaster Recovery Procedures for a sample of quarters to confirm the Disaster Recovery Procedures are tested on a semi-annual basis.	No exceptions noted.
CC9.1.3	Recovery time objectives (RTOs) are identified for the technologies supporting the system and are documented in customer agreements.	Inspected the contracts for a sample of new customers to confirm the RTOs are identified for the technologies supporting the system and are documented in customer agreements.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC9.1.4	Threats that could cause a business disruption are documented in a risk assessment. The threats are assessed for likelihood and impact.	Inspected the Risk and Improvement Register to confirm threats that could cause a business disruption are documented in a risk assessment and the threats are assessed for likelihood and impact.	No exceptions noted.
CC9.1.5	The Company has purchased insurance policies to offset the financial impact of business disruptions, including disruptions arising from cyber events.	Inspected the insurance policy to confirm the Company has purchased insurance policies to offset the financial impact of business disruptions, including disruptions arising from cyber events.	No exceptions noted.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	The Supplier Management Policy defines expectations for identifying and risk rating all vendor relationships. The risk ratings consider the access to the Company's data and the criticality of the vendor to providing services.	Inspected the Supplier Management Policy to confirm the policy defines expectations for identifying and risk rating all vendor relationship and the risk ratings consider the access to the Company's data and the criticality of the vendor to providing services.	No exceptions noted.
CC9.2.2	The vendor risk assessment rates the risk of a vendor based on access to the Company data and the criticality of the vendor.	Inspected the vendor risk assessment to confirm the vendor risk assessment rates the risk of a vendor based on access to the Company data and the criticality of the vendor.	No exceptions noted.
CC9.2.3	Subservice organizations are reviewed on an annual basis.	Inspected the annual reviews for the subservice organizations to confirm subservice organization are reviewed on an annual basis.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
CC9.2.4a	The Supplier selection process includes a review of materials to ensure the risks associated with the vendor relationship are understood. A Supplier Agreement Form is completed for the selected new vendors to document the risks associated with the new relationships.	Inspected the Supplier Management Policy to confirm the Supplier selection process includes a review of materials to ensure the risks associated with the vendor relationship are understood.	No exceptions noted.
CC9.2.4b		Inspected the Supplier Agreement Form for a sample of new vendors to confirm the supplier selection process includes a review of materials to ensure the risks associated with the vendor relationship are understood and a Supplier Agreement Form is completed for the selected new vendors to document the risks associated with the new relationships.	No exceptions noted.
A1.0 - Additional Criteria for Availability			
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1a	Solutions are configured to collect logs of performance and capacity metrics. The solutions are configured to monitor capacity and availability metrics for the system including disk usage, memory usage, processor load, and server downtime/ uptime. An alert is generated to appropriate personnel when defined performance metrics are exceeded.	Inspected the configurations of the solutions to confirm the solutions are configured to collect log and to monitor capacity and availability metrics for the system including disk usage, memory usage, processor load, and server downtime/uptime.	No exceptions noted.
A1.1.1b		Inspected the configurations of the solutions to confirm appropriate individuals are alerted when defined performance metrics are exceeded.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
A1.1.1c		Inspected example alerts to confirm alerts are generated to appropriate personnel when defined performance metrics are exceeded.	No exceptions noted.
A1.1.2a	The Incident Management Team meets on a weekly basis to discuss incidents that occurred that impacted system performance and capacity. The Incident Management Team will evaluate the need for additional technologies and resources.	Inquired with management to confirm the Incident Management Team meets on a weekly basis to discuss incidents that occurred that impacted system performance and capacity and evaluate the need for additional technologies and resources.	No exceptions noted.
A1.1.2b		Inspected the Incident Management Team meeting invite for a sample of weeks to confirm the Incident Management Team meets on a weekly basis to discuss incidents that occurred that impacted system performance and capacity and evaluate the need for additional technologies and resources.	No exceptions noted.
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.			
A1.2.1a	All production data is backed up on at least a daily basis. All backups are encrypted while in transit and at rest. All backup data is retained for at least thirty (30) days.	Inspected the Backup and Restore Policy to confirm all production data is backed up on at least a daily basis and retained for thirty (30) days.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
A1.2.1b		Inspected the backup configurations to confirm all production data is backed up on at least a daily basis, retained for thirty (30) days, and is encrypted while in transit and at rest.	No exceptions noted.
A1.2.2a	Appropriate personnel are notified of failures or errors during the backup process for investigation.	Inspected the backup configurations to confirm appropriate personnel are notified of failures or errors during the backup process for investigation.	No exceptions noted.
A1.2.2b		Inquired with management to confirm there were no AWS backup failures to verify appropriate personnel are notified during the audit period. Therefore, the Service Auditor was unable to test the operating effectiveness of the control during the audit period.	Control did not operate during the period.
A1.2.2c		Inspected an example Azure alert to confirm appropriate personnel are notified of failures or errors during the backup process for investigation.	No exceptions noted.
A1.2.3a	Backup restore tests are performed on a semi-annual basis to validate the integrity of data backups.	Inspected the Backup Procedure to confirm backup restore tests are performed on a semi-annual basis to validate the integrity of data backups.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
A1.2.3b		Inspected the most recent backup restore tests to confirm backup restore tests are performed on a semi-annual basis to validate the integrity of data backups.	No exceptions noted.
A1.2.4	Controls related to the environmental protections of the facilities hosting assets and infrastructure supporting their services are the responsibility of the subservice organizations AWS and Microsoft. See the Complementary Subservice Organization Controls above for additional details.		
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1a	Backup restore tests are performed on a semi-annual basis to validate the integrity of data backups.	Inspected the Backup Procedure to confirm backup restore tests are performed on a semi-annual basis to validate the integrity of data backups.	No exceptions noted.
A1.3.1b		Inspected the most recent backup restore tests to confirm backup restore tests are performed on a semi-annual basis to validate the integrity of data backups.	No exceptions noted.
A1.3.2	The Business Continuity Plan and Disaster Recovery Procedures addresses recovering connectivity and supporting systems to ensure customer obligations can be met.	Inspected Business Continuity Plan and Disaster Recovery Procedures to confirm the policies and procedures address recovering connectivity and supporting systems to ensure customer obligations can be met.	No exceptions noted.

Key	Service Organization Controls	Tests	Results
A1.3.3a	The Business Continuity Plan is tested by the Company on an annual basis and the Disaster Recovery Procedures are to be tested on a semi-annual basis.	Inspected the Business Continuity Plan and Disaster Recovery Procedures to confirm the Business Continuity Plan is tested by the Company on an annual basis and the Disaster Recovery Procedures are to be tested on a quarterly basis.	No exceptions noted.
A1.3.3b		Inspected the annual Business Continuity Plan test results to confirm the Business Continuity Plan was not tested during the audit period.	No exceptions noted.
A1.3.3c		Inspected the testing for the Disaster Recovery Procedures for a sample of quarters to confirm the Disaster Recovery Procedures are tested on a semi-annual basis.	No exceptions noted.
A1.3.4	Controls related to implementing and testing recovery plan procedures are the responsibility of the subservice organizations AWS and Microsoft. See the Complementary Subservice Organization Controls above for additional details.		

V. ADDITIONAL INFORMATION PROVIDED BY PRESERVICA, INC.

A. CONTROL EXCEPTIONS AND PRESERVICA, INC.'S MANAGEMENT RESPONSES

The following section contains Preservica, Inc.'s detailed responses to the control exceptions discovered by Wolf & Company, P.C. covering the period of October 1, 2021 to September 30, 2022.

Applicable Trust Services Criteria	Service Organization Control	Exception Noted	Management Response
CC1.2.2b CC2.1.2b CC4.2.6b	The Leadership Team meets on a weekly basis to discuss operational action items, issues, etc. Additionally, the Team meets monthly to discuss strategic plans and updates.	The weekly Leadership Team Meeting did not occur in two (2) of the five (5) sampled weeks.	In addition to the weekly Leadership Team (LT) meetings, there are monthly Strategy meetings. The weekly LT meetings are block booked for the year in advance but do not occur when the Strategy meeting is held. A Strategy meeting was held on the two sampled weeks that did not have an LT weekly meeting.
CC1.4.2	The Company performs several checks on prospective employees, including credit, education, and references.	One (1) of the three (3) sampled new hires did not have credit and reference checks prior to hire.	Occasionally if an employee is hired at short notice, there is not time to get all the background checks done before they start employment. These checks are then completed as soon as possible after they commence work. Earlier this year, we hired a full time HR Manager to improve our onboarding of employees including background checks etc.

Applicable Trust Services Criteria	Service Organization Control	Exception Noted	Management Response
CC3.4.2 CC5.3.2	Policies and procedures are reviewed on an annual basis and updated, as needed.	The Product Development Policy in effect for the audit period has not been formally approved since August 2021.	This document was on an 18-month review cycle and was not due for review until end December 2022. We now have a policy in place ensuring that all documents will be reviewed on an annual review basis.
CC6.2.5b CC6.3.5b	Written authorization is required is required to request granting system access for all new consultants and removal for all terminated consultants.	One (1) terminated consultant did not have access revoked in a timely manner.	Manager did not inform the IS department that the consultant had left. All managers have been reminded of their responsibility and the process that needs to be followed when consultants leave.