HRACUITY®

Report on HR Acuity, LLC’s Description of the Employee Relations Services System and the Suitability of the Design and Operating Effectiveness of Controls for the Period April 1, 2021 through March 31, 2022 Relevant to Security

SOC 2®

IS Partners
Audits Without Anxiety®

This report is not to be copied or reproduced in any manner without the expressed written approval of HR Acuity, LLC. The report, including the title page, table of contents, and exhibits, constitutes the entire report, and should be referred to only in its entirety and not by its component parts. The report contains proprietary information and is considered confidential.

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of HR Acuity, LLC:

Scope
We have examined HR Acuity, LLC's ("HR Acuity") accompanying description of its Employee Relations Services system titled "HR Acuity, LLC's Description of the Employee Relations Services System" throughout the period April 1, 2021 through March 31, 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 April 1, 2021 through March 31, 2022, to provide reasonable assurance that HR Acuity's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

HR Acuity uses subservice organizations to provide infrastructure hosting cloud services and asset related management in support of the HR Acuity system. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at HR Acuity, to achieve HR Acuity's service commitments and system requirements based on the applicable trust services criteria. The description presents HR Acuity's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of HR Acuity's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at HR Acuity, to achieve HR Acuity's service commitments and system requirements based on the applicable trust services criteria. The description presents HR Acuity's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of HR Acuity'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
HR Acuity is responsible for its service commitments and system requirements and for designing and implementing controls within the system to provide reasonable assurance that HR Acuity's service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that HR Acuity's service commitments and system requirements were achieved. HR Acuity has provided the accompanying assertion titled "HR Acuity, LLC's Management Assertion"

("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. HR Acuity 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 the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and 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.

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

Inherent limitations
The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of tests of controls
The specific controls we tested, and the nature, timing and results of those tests are presented in section VII.

Opinion
In our opinion, in all material respects:

a. The description presents HR Acuity, LLC's Employee Relations Services System that was designed and implemented for the period April 1, 2021 through March 31, 2022, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period April 1, 2021 through March 31, 2022, to provide reasonable assurance that HR Acuity'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 HR Acuity's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period April 1, 2021 through March 31, 2022, to provide reasonable assurance that HR Acuity'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 HR Acuity's controls operated effectively throughout that period.

Restricted use
This report, including the description of tests of controls and results thereof in section VII, is intended solely for the information and use of HR Acuity, user entities of HR Acuity's Employee Relations Services System during some or all of the period April 1, 2021 through March 31, 2022, business partners of HR Acuity subject to risks arising from interactions with

the employee relations 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.

IS Partners, LLC

IS Partners, LLC
Dresher, Pennsylvania
May 9, 2022

IS PARTNERS LLC • CERTIFIED PUBLIC ACCOUNTANTS •
SECURITY · AVAILABILITY · PROCESSING INTEGRITY · CONFIDENTIALITY · PRIVACY
SOC 2®

II. HR ACUITY, LLC'S MANAGEMENT ASSERTION

We have prepared the accompanying description of HR Acuity, LLC's ("HR Acuity") "Description of HR Acuity's, LLC's Description of the Employee Relations Services System" throughout the period April 1, 2021 through March 31, 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 Employee Relations Services System that may be useful when assessing the risks arising from interactions with HR Acuity's system, particularly information about system controls that HR Acuity has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, (AICPA, *Trust Services Criteria*).

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

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

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

a. The description presents HR Acuity's Employee Relations Services System that was designed and implemented throughout the period April 1, 2021 through March 31, 2022, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period April 1, 2021 through March 31, 2022, to provide reasonable assurance that HR Acuity'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 subservice organizations and user entities applied the complementary controls assumed in the design of HR Acuity's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period April 1, 2021 through March 31, 2022, to provide reasonable assurance that HR Acuity’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 HR Acuity’s controls operated effectively throughout that period.

III. HR ACUITY, LLC'S DESCRIPTION OF ITS EMPLOYEE RELATIONS SERVICES SYSTEM

Background

HR Acuity ("HRA") is a privately held, women-owned company founded in 2006 to provide software- as-a-service (SaaS) for employee relations. HR Acuity provides an end-to-end employee relations technology solution designed to consolidate manual employee relations processes, centralize employee relations data, ensure consistency, and drive process through integrated HR best practices, and real time data in the form of trends and reports. As a result, organizations are able to efficiently manage issues and mitigate risk with a solution that is designed specifically for employee relations.

HR Acuity currently has more than 30 team members, has more than 125 customers and has its headquarters in Florham Park, New Jersey. The headquarters in New Jersey is responsible for the key business area, operations, overall success of the corporation and ensuring corporate governance. Key sales team members are located throughout the United States. In addition to those located in New Jersey, HR Acuity leverages development resources in both Mumbai and New Delhi, India.

Services Provided

In today's world, organizations are at a greater risk of financial, reputational, and cultural damage from employee events that go mismanaged. With the #MeToo movement and countless organizations hitting the press for harassment allegations, there is a tremendous spotlight on HR to show that incidents are being addressed in a timely and compliant manner. Not only is it important to have the proper procedures in place, but it is equally important to have the right tools to monitor these events and respond accordingly.

State of Case Management Today and Intended Results

Most organizations today use a variety of manual processes to manage their employee relations issues. Some use spreadsheets, shared drives, and paper files, others attempt to retrofit an existing system (like their HRIS or compliance software) to track issues. The problem with using systems that are not dedicated to the function is that the organization opens itself up to risk. There is risk in not having the data in one place to spot trends and monitor issues, there is risk in handling issues in an inconsistent way, and there is risk in confidential data being exposed.

Organizations also struggle with data loss when a member of the HR team leaves or moves in the organization, because most details are stored in notebooks, or in a form that cannot be reported on easily. Also, there are obvious efficiency challenges that most HR teams face with a manual process.

HR Acuity application has an employee relation module which allows organizations to handle and document non-investigation related issues (e.g., benefits and leave related items, performance, policy deviations, etc.) Investigation Methodology: This is for managing serious allegations that require an investigation and potential legal intervention. Users are able to conduct investigations from start to finish in this module and will be guided in how to conduct the investigation with HR best practices.

HR Acuity also allows the organization and users to weave together the employees' history and serve up real time insights through trends and report.

Admins also are able to control user permissions so certain items remain confidential.

HR Acuity also provides a variety of other features to aid HR departments in effectively managing employee matters. They include:

- Post Hire and Exit Interviews
- Web Forms to electronically intake issues from employees
- Queue to integrate with hotlines and other ticket management systems, and
- Manager Portal for issues tracking and management at the People Manager level

Principal Service Commitments and System Requirements

HR Acuity is committed to high standards of excellence for the protection of information assets and information technology resources that support the HR Acuity environment. HRA processes, stores, and transmits electronic information to conduct its business functions. Without the implementation of appropriate controls and security measures, these assetswould be subject to potential damage or compromise to Confidentiality, Integrity and Availability, and the activities of HR Acuity and its clients would be subject to interruption.

The purpose of the Information Security Policy is to set forth the underlying tenets, framework, and reasoning for the HR Acuity Information Security Management System (ISMS) in accord with the requirements of ISO standard ISO/IEC 27001:2013., as well as state privacy security laws and regulations in the jurisdictions in which HR Acuity operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other client agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following: Security principles within the fundamental designs of the HR Acuity applications are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

HR Acuity establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in HR Acuity's system policies and procedures, system design documentation, and contracts with clients. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the HR Acuity applications

Components of the System

The system is comprised of the following five components:

- Infrastructure (systems and networks)
- Software (web application & utilities)
- People (Engineers, IT project managers, Product Manager)
- Procedures (automated and manual)
- Data (transactions streams, files, databases, and storage)

The following sections of this description define each of these five components comprising the HR Acuity system and other relevant aspects of HR Acuity's control environment, risk assessment process, information and communication systems, and monitoring controls.

Infrastructure and Software

HR Acuity partners with Microsoft Azure ("MS Azure") to provide infrastructure hosting cloud services in support of the HR Acuity system. The solution is developed using the Microsoft software stack and adheres to the Microsoft.Net MVC pattern-based framework that enables a clean separation of concerns and provides full control for creating sophisticated features that use the latest web standards. HR Acuity's systems and applications are configured in redundant configurations to provide availability in the event of system failure. HR Acuity environment consists of development, QA, UAT, Staging, Production and Disaster Recovery instances. These instances are hosted on MS Azure ASE cloud environment. HR Acuity databases are hosted on MS Azure data centers in south-central and north-central United States. Servers are configured according to predefined secure configuration standards that aim to protect HR Acuity's systems and applications from unauthorized access and disclosure of confidential information. All infrastructure is subject to regular vulnerability testing and undergoes external penetration testing annually to ensure the highest level of security and data integrity.

The following table describes hardware and software specifications in the HR Acuity environment for the applications/systems in-scope for this report:

Application/ System	Process/Transactions	Purchased or Developed	Platform and Operating System	Data Environment
HR Acuity Web Application	SaaS-based employee relations technology solution used by organizations to achieve consistency in the way they track, investigate, and analyze employee issues.	Developed Internally	MS Azure ASE	MS Azure
Analytics Engine	This system is used to integrate web application and analytics application.	Developed Internally	MS Azure VM	MS Azure
Emailer and Notification Application	This system is a backend application that is used to integrate emails and user notifications.	Developed Internally	MS Azure VM	MS Azure
HR Acuity REST based API	REST based API provides support to iPhone/ iPad applications.	Developed Internally	MS Azure VM	MS Azure
iPad HR Acuity Application	Users of HR Acuity can use iPad application to track, investigate and analyze employee issues.	Developed Internally	Apple App Store	MS Azure

Application/ System	Process/Transactions	Purchased or Developed	Platform and Operating System	Data Environment
iPad/ iPhone HR Acuity Manager's Access Application	This application is used by Manager users to document Employee Relation issues.	Developed Internally	Apple App Store	MS Azure
SFTP Upload application.	This application is used for uploading employee, group and location data provided by HR Acuity clients on a scheduled basis.	Developed Internally	MS Azure VM	MS Azure

A demilitarized zone (DMZ) network separates inbound traffic from the internet and production servers placed in operation at the HR Acuity MS Azure environment. Redundant backup of data is being performed and stored with in United States to provide availability of the applications or data in the event of a system failure. Strong authentication policies are required to access network equipment. Written hardening policies and procedures are in place for the deployment of servers, firewalls, and routers at the MS Azure data center.

People

HR Acuity is led by a team of employee relations and technology experts with a vision for a better employee relations process. HR Acuity's leadership team is dedicated to doing things the right way – no matter what it takes, no matter how difficult. HR Acuity goes above and beyond to ensure their solutions continue to equip their customers with the technology and expertise they need to protect their people and their organizations.

Various departments exist within HR Acuity to organize and focus work efforts.

The leadership team is responsible for the control environment for the organization and comprises knowledgeable and experienced executives working on establishing the appropriate tone at the top.

As a privately held company, HR Acuity has a senior management team that meets to review, approve and advise on corporate plans and policies, and to monitor HR Acuity's progress. The senior management team reviews and approves corporate plans and policies as related to managing assets, risk and organizational, financial and operating key performance indicators.

The Senior Management team of HR Acuity is as follows:

- Deborah Muller, CEO & Privacy Officer
- Paul Witherspoon, VP of Technology
- Kevin Herendeen, CFO
- Greg Fraser, CPO
- Beth Prunier, SVP of Sales
- Michael Rubino, Director of Customer Support and Professional Services

The HR Acuity Information Security Management System (ISMS) Steering Committee is as follows:

- Deborah Muller, CEO & Privacy Officer
- Paul Witherspoon, VP of Technology
- Kevin Herendeen, CFO
- Joe Stock, DPO
- Paul Witherspoon, ISMS Manager

The IT department reports up to the Chief Technology Officer (CTO & ISO); however, the HR Acuity Leadership Team is responsible for setting the strategic direction for the security of the systems that support the enterprise. The VP of Technology, in cooperation with the HR Acuity leadership team, is ultimately responsible for the security of data and assets of HR Acuity and ensuring that a consistent, well-supported and effective security program is implemented and maintained.

The leadership team is made up of the following individuals:

- CEO
- VP (Technology) & ISO
- CPO
- CFO
- SVO (Sales)
- VP (Professional Services)
- VP (Marketing)
- Director (Customer Support)

Information Technology

The IT department is responsible for the control of general computer operations, the maintenance of existing systems, the acquisition and implementation of new systems, and the management of physical and information security at HR Acuity's processing facilities. Key responsibilities in the IT department include:

Windows System Engineers

The Windows system engineers are responsible for the administration, availability and deployment of server hardware, Microsoft Windows operating systems, back-office services and business-critical applications. They perform administration tasks and Tier 2 and 3 level support for a wide array of enterprise technology solutions.

Operation Backup Engineers

The operation backup engineers are responsible for the design, administration, management and engineering of the global backup strategy and the creation of technical documentation related to system configurations, processes, procedures and knowledge base articles and provide mentoring and coaching and other infrastructure resources to team members.

Senior Security Engineers

The senior security engineers are responsible for the design, deployment and administration of security implementations and practices. They perform security incident and event management investigations to resolution and perform risk, threat and vulnerability management assessment functions.

Administration

The Administration department is responsible for the development of personnel practices and for verifying compliance with personnel policies and procedures throughout the organization. In addition, they are responsible for financial activities of HR Acuity, including corporate financial planning and accounting and regional accounting for the processing facilities.

Sales

The Sales Organization is responsible for product demos, pricing, feature review and sales negotiations as prospects transition to clients.

Client Success

The Client Success organization is responsible for the on-boarding, training, support and account management of all clients.

Procedures

The HR Acuity system's technical documentation is available to authorized personnel. The system has documentation for systems, programming, operations, security and users of the system. Technical documentation is maintained or developed by the technology departments and provided to appropriate personnel and users. The technical documentation describes the role and responsibilities of the technical staff responsible for developing HR Acuity technology solutions and support, a system overview of how HR Acuity applications are built, the services provided by HR Acuity, a high-level data model of key functional areas of HR Acuity applications, the technology used to build HR Acuity applications, the development tools and methodologies to transform system/business requirements into HR Acuity technology deliverables, key interfaces used to fulfill system requirements, the delivery mechanisms used to build and deploy HR Acuity applications, the authentication and authorization mechanisms used to validate who can do what in the applications, the reporting strategy used with HR Acuity applications and how to troubleshoot HR Acuity applications build and runtime issues. The aforementioned Company policies and procedures are available to users of the HR Acuity system.

Data

HR Acuity's system data includes electronic information entered into the systems through multiple formats: Microsoft Excel, comma-separated values, or data entry from the client. Clients send this data by a variety of methods, including a HR Acuity Secure File Transfer Protocol (SFTP). The data is loaded and stored in the Azure SQL Databases database that corresponds to the respective HR Acuity application. The HR Acuity system does not have access to confidential client data containing sensitively identifiable information unless provided by the client as part of custom information. HR Acuity leverages MS Azure datacenters in continental United States. These geographically dispersed datacenters comply with key industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, for security and reliability. The datacenters are managed, monitored, and administered by Microsoft operations staff 24/7/365.

Data as defined by the systems includes the following:

- Employee data including employee id, first name, last name, and email for application users. Additional data may be provided by the clients.
- Case data including notification date, notification method, group, location, issues, and actions.
- Case attachments including relevant policies, emails, and other case related items.
- User access and permission data including case entry, view, and reporting permissions.
- Client organizational data including locations and organizational hierarchy.
- Survey response data including employee post hire and exit interview responses.

HR Acuity is responsible for assuring proper use of the data through documented policies and procedures, enforces separation of duties and the principle of least privilege when granting access.

IV. OTHER RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION SYSTEMS, AND MONITORING CONTROLS

The management of HR Acuity has established a system of internal controls aligned with the integrated framework established by the Committee of Sponsoring Organizations ("COSO"). The following processes describe management's approach to addressing the COSO integrated framework.

Control Environment

HR Acuity is committed to maintaining an organizational structure that supports an effective control environment. The control environment is comprised of various elements, including the proper segregation of job responsibilities, assignment of job functions commensurate with skill, properly defined roles and responsibilities, hiring of experienced staff, internal quality control processes, management oversight, and proactive fraud detection and risk mitigation strategies, established to facilitate the effectiveness and integrity of HR Acuity operations.

Risk Assessment Process

HR Acuity has developed and implemented a risk-based information security program to provide a baseline security overview and recommendations on how the information security risks should be addressed. The goal of the program is to ensure that systems are secure and properly administered and adhere to security guidelines. On an annual basis, management performs a risk assessment that includes the HR Acuity system that identifies and analyzes the significance of potential threats that would impair system security, as well as determining mitigation strategies for those risks. The results are used to provide recommendations on how risks should be addressed and develop strategies to mitigate the risks identified.

The operations department holds weekly meetings to discuss changes related to system security, as well as the design and operating effectiveness of controls. A formal vulnerability management policy is included in the information security policy, which is reviewed, updated if needed, and approved on an annual basis by the management. HR Acuity maintains a formal business continuity and disaster recovery plan, which are reviewed, updated if needed and approved on an annual basis by the management.

Annually, management performs an external vulnerability assessment to adequately identify potential risks. Issues identified are reviewed, and actions are taken to adequately mitigate the identified risks.

Information and Communication Systems

<u>Internal Communication</u>
HR Acuity communicates to internal employees and external system users through various methods. A corporate intranet site is available to internal employees for Company policies and procedures, and significant events. For external system users, system manuals are available on request, and the corporate website is available for additional resources forthe applications or general Company questions.

External Communication

HR Acuity's security commitments are communicated to external system users on its privacy statement, which is posted on HR Acuity website. The client statement of work agreement includes HR Acuity's obligations and the systems boundaries to maintain system security for external system users. HR Acuity maintains a formal networkdiagram for internal users, which illustrates the system and its boundaries.

Clients are notified of changes to the systems and its boundaries by posting a message on the HR Acuity web portal. Technical guidelines, including the system description and boundaries, are available to clients via client requests. Changes to the system and its boundaries are communicated to HR Acuity employees through a maintenance schedule, which is emailed to a distribution group notifying them of the maintenance.

Monitoring Controls

Management meets regularly to plan and monitor business and operations. The Executive Committee and the security group meet at least twice per year to review technology policies, risks, operations, processes and the technology needs of the entire organization.

Monitoring tools are in place to monitor, identify and report to appropriate personnel incidents related to the introduction of unauthorized or malicious software, and to unauthorized attempts to access or disrupt the network. The IT department is responsible for monitoring the performance and availability of the infrastructure and HR Acuity system.

Firewalls are placed in operation on critical network connections, including the internet. WAF (Web Application firewalls) are configured to protect system infrastructure from unauthorized or malicious software. Firewalls are configured to accept trusted sources and deny other sources. A demilitarized zone (DMZ) is implemented to separate traffic from the web to internal networks and devices.

Network monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs and unusual system activity. An intrusion detection system (IDS) is put in place by HR Acuity to monitor, identify and report to appropriate personnel incidents related to the introduction of unauthorized or malicious software and unauthorized attempts to access or disrupt the network. HR Acuity implements WAF and SIEM solution to monitor/ secure web traffic. HR Acuity Security Operations Center monitors incoming traffic 24/7/365. This highly skilled security team (former leaders of the Israeli cyber security defense team) provides expert monitoring, investigation, mitigation, forensics to proactively ensure the security of our network and client data. The Incident Response Team will provide immediate, effective and skillful response to any critical cyber incident and DDoS attacks. Files uploaded by the users are checked for both integrity and virus definitions.

Annually, management performs an external vulnerability assessment to adequately identify potential risks. Issues identified are reviewed, and actions are taken to adequately mitigate the identified risks.

Logical and Physical Access Controls

HR Acuity maintains policies that manage access to applications, systems, hardware, and the execution of automated functions. These policies encompass all HR Acuity employees, clients, vendors, contractors, consultants, temporaries, and other non-employee staff requiring access.

HR Acuity policies dictate the process of requesting and assigning logical access rights. Logical access is provisioned according to the principle of least privilege. Only the minimum level of access to infrastructure and systems needed per job responsibilities is granted. The duties related to the creation of access rights are segregated between the individual with authority to determine who has access to systems and data and the individual assigning the access rights to minimize the risk of fraudulent activity. HR Acuity uses role-based group access to restrict access to system resources and restricts access to the resources to the users granted permissions to that respective resource based on job responsibilities and/or relationship to the entity. Privileges assigned shall be limited to the minimum required to perform assigned duties and in accordance with the Information Security Policy. All access not explicitly authorized is forbidden.

HR Acuity maintains a policy that establishes a general minimum standard for passphrases and passwords that includes the creation of strong passphrases and passwords, protection of passphrases/ passwords, and the frequency of renewing passphrases/passwords. The policy applies to all individuals, employees and non-employees, who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any HR Acuity facility, has access to the network, or stores any non-public information.

Resetting, deleting, and modifying passwords or user IDs, credentials, and other identifier objects must only be done by authorized members of the Information Technology team. The IT staff is required to verify the user’s identity before resetting a passphrase or password and monitoring for and deactivating inactive user accounts at least every 90 days is required.

HR Acuity maintains policies that support appropriate physical access controls for its headquarters, datacenter hosted on MS Azure. The policy defines the requirements for protecting company information and technology resources from physical and environmental threats in order to reduce the risk of loss, theft, damage, or unauthorized access to those resources, or interference with HR Acuity operations.

Guests, clients, vendors, contractors, consultants, temporaries, and non-employee other staff are issued a building access card based on need determined by HR Acuity management. Building access is segregated by role and relationship to the entity.

The company headquarters is equipped with environmental protections including internal cameras, fire protection and backup power for critical systems. All doors are locked and only accessible via key cards.

Change Management

HR Acuity embeds security controls in the S-SDLC process to ensure security throughout the development process and provides resources for security assessment, testing and review.

- Manual code reviews are done before any code merge to the Master branch.
- Static Analysis Security Analysis (SAST) is performed using Veracode during the development process to identify and remediate any security vulnerabilities before production release.
- Dynamic Analysis Security Analysis (DAST) is performed on the runtime environment to find any OWASP 3.0 related vulnerabilities.
- Targeted manual security testing is performed by product security engineers based on the highest identified risks in security risk assessment
- At least annually, HR Acuity engages with a third-party world class application security firm to perform automated and manual penetration testing and dynamic analysis.
- Continuous assessment of global security and compliance across web applications and cloud infrastructure is managed using external vulnerability management solution.
- To ensure ongoing security awareness, HR Acuity security engineers meet regularly to share knowledge on emerging trends and threats and to evangelize best practices and raise overall awareness related to site security throughout the organization.

Security Incidents during the Period

HR Acuity has a well-established incident management program that consists of documented incident response plans, a dedicated Information Technology team and Information Security team.

HR Acuity diligently responds to alerts received from various monitoring tools deployed at the perimeter of the network, within the network and applications. During the course of the audit period, HR Acuity investigated a few incidents related to its systems and applications performance and security controls. These incidents were promptly responded to and mitigated.

None of the incidents led to an actual data breach or were significant enough to trigger external communications. An example of such incidents is malware detected on a server where customer data is not hosted.

Changes to the System during the Period

There were no changes that are likely to affect report users’ understanding of how the HR Acuity platform is used to provide the service during the period from April 1, 2021 through March 31, 2022.

V. SUBSERVICE ORGANIZATIONS

HR Acuity uses subservice organizations to perform various functions to support the delivery of services. The scope of this report does not include the controls and related trust services criteria at the subservice organization. The following table describes the services provided by the subservice organization:

Subservice Organization	Services Provided
Microsoft Azure ("MS Azure")	HR Acuity uses MS Azure to provide infrastructure hosting cloud services in support of the HR Acuity systems and applications
TechWerxe	HR Acuity uses TechWerxe for asset related management including, monitoring, patching, whitelisting, and installing applications.

Below are the applicable trust services criteria that are impacted by the subservice organizations and the controls expected to be implemented at the subservice organizations to meet the applicable criteria:

Applicable Trust Services Criteria	Subservice Organization Controls Expected to be Implemented to Meet the Applicable Trust Services Criteria
CC 6.1 – 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.	• Logical access to offline storage, backup data, systems and media requires authorization, and access is reviewed periodically. • Firewalls and intrusion prevention systems are used and configured to prevent unauthorized access. The events are logged and reviewed. • Intrusion detection systems (IDS) are in place to monitor Web traffic and identify potential patterns or threats. • All access to system components requires that users are authenticated through unique user IDs and passwords. • Logical access to offline storage, backup data, systems and media requires authorization, and the access should be reviewed periodically.
CC 6.2 – 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.	• An Information Security Policy includes the standards for logical security tools and techniques restricting access to applications, systems and data. • Access to applications, systems and data is restricted to users with a valid business need and supported by a documented approval. • Privileged access to applications, systems and data is restricted to users with a valid business need. • Access to applications, systems and data is reviewed on a periodic basis.

Applicable Trust Services Criteria	Subservice Organization Controls Expected to be Implemented to Meet the Applicable Trust Services Criteria
CC 6.3 – The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	• Access to applications, systems and data is restricted to users with a valid business need and supported by a documented approval. • Privileged access to applications, systems and data is restricted to users with a valid business need. • Access to applications, systems and data is reviewed on a periodic basis. • System access rights of terminated users are removed upon notification.
CC 6.4 – 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.	• Physical access to the data center facilities, backup media and other system components, such as firewalls, routers and servers, requires authorization, and this access should be reviewed. • Individuals are required to swipe their electronic access card reader in order to enter a restricted facility such as the data center and other sensitive areas. Individuals are required to display their employee or visitor ID cards while in a restricted facility. • Visitors are required to sign in and undergo authorization processes upon entering the building.
CC 6.5 – 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.	• On a monthly basis, the security team reconciles active badges against a list of active employees and contractors to validate that access to the data center and other sensitive areas is restricted based on job responsibilities. • System access rights of terminated users are removed upon notification.
CC 7.2 – 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.	• Firewalls and intrusion prevention systems are used and configured to prevent unauthorized access. The events are logged and reviewed. • Intrusion detection systems (IDS) are in place to monitor Web traffic and identify potential patterns or threats.
CC 7.3 – 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.	• Scheduled tasks that do not process as expected are followed-up daily and resolved. • Intrusion detection systems (IDS) are in place to monitor web traffic and identify potential patterns or threats. • Operations and security personnel follow defined protocols for resolving and escalating reported events.
CC 7.4 – The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	• Scheduled tasks that do not process as expected are followed-up daily and resolved. • Intrusion detection systems (IDS) are in place to monitor web traffic and identify potential patterns or threats. • Operations and security personnel follow defined protocols for resolving and escalating reported events.

Applicable Trust Services Criteria	Subservice Organization Controls Expected to be Implemented to Meet the Applicable Trust Services Criteria
CC 7.5 – The entity identifies, develops, and implements activities to recover from identified security incidents.	• Operations and security personnel follow defined protocols for resolving and escalating reported events.

Monitoring of Subservice Organizations

HR Acuity uses service organizations to provide certain expertise. HR Acuity's subservice organizations are annually assessed to determine if they perform services for HR Acuity relevant to the SOC 2 criteria used by the company to create its own annual SOC 2 audit report. For those subservice organizations deemed to provide relevant services, they are further analyzed to determine if the services provided warrant the requirement to provide their own SOC 2 report to HR Acuity for the services and service periods relevant to their operations with HR Acuity.

In addition to obtaining SOC 2 reports, HR Acuity monitors subservice organizations throughout the contract periods by maintaining close working relationships with the subservice organizations. HR Acuity reviews subservice outputs to ensure contract compliance, effectiveness, and cost-beneficial acquisition of the contracted services. Any discrepancies noted between actual output received and management's expectations are investigated and addressed with the subcontractor for additional action. HR Acuity maintains monthly reporting from TechWerxe as part of the contract and all reports are reviewed by management to address any issues identified.

VI. COMPLEMENTARY USER ENTITY CONTROLS

HR Acuity’s controls surrounding the Employee Relations Services System were designed with the assumption that certain controls would be placed in operation at user organizations. In certain instances, the application of specific controls at user organizations is necessary to achieve certain Trust Services Criteria included in this report.

The following list outlines controls that should be in operation at user organizations to complement the controls listed in section VII. The list does not represent a comprehensive set of all controls that should be employed by user organizations. User auditors should consider whether the following controls have been placed in operation at user organizations:

- The user organization should have policies and controls implemented for creating user credentials, assigning appropriate roles, reviewing user access and timely revoking user access of their users within HR Acuity’s application.

- The user organization should have policies and controls implemented to control and monitor the type of data they input in the application, the accuracy of the data they input, choose the right fields / field types for data input and the consequent impact of any unnecessary sensitive data input in the systems.

- The user organization should have policies and controls for the use of passwords related to their User IDs used to access the application if they opt for integrating with their own SSO or where the application allows to customize the password policies.

- The user organization should have policies and controls implemented to ensure only the required data is configured to be made public using the available configurations in HR Acuity’s application. User organization should have proper controls such as approvals if they choose to make PII data public.

- The user organization should have procedures to ensure that timely notifications of terminated agreements are provided to HR Acuity, and if there are any requirements for data deletion prior to the agreement termination.

- The user organization should have procedures to ensure that only authorized employees have the ability to access data.

- Controls should be established to ensure that all data transmitted by the user organizations to HR Acuity is complete, accurate, timely, and protected.

VII. INDEPENDENT SERVICE AUDITOR’S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

Introduction

The trust services criteria relevant to *Security* address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

Security refers to the protection of

i. information during its collection or creation, use, processing, transmission, and storage, and
ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

SECURITY

CONTROL ENVIRONMENT

CC1.1: The entity demonstrates a commitment to integrity and ethical values.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC1.1.1	Management monitors employees' compliance with the code of conduct through monitoring of performance and employee’s complaints.	For a sample of new hires, obtained and inspected the signed copy of the code of conduct document to determine that management monitors employees' compliance with the code of conduct through monitoring of performance and employee’s complaints.	No exceptions noted.
CC1.1.2	Personnel are required to read and accept the code of conduct and the privacy practices upon their hire.	For a sample of new hires, obtained and inspected a copy of the signed privacy practices for new hires to determine employees are required to read and accept the code of conduct and the privacy practices upon their hire.	No exceptions noted.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC1.1.3	Personnel must pass a criminal background check before they may be hired by the entity or third-party vendors hired by the entity.	For a sample of new hires, obtained and inspected evidence of background checks performed to determine that personnel must pass a criminal background check before they may be hired by the entity or third-party vendors hired by the entity.	No exceptions noted.
CC1.1.4	Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.	Obtained and inspected the Vendor Management Security Standard to determine that a procedure for evaluating adherence to those security standards and addressing deviations in a timely manner was in place.	No exceptions noted.

CC1.2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC1.2.1	The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.	Obtained and inspected documents of the board of directors with their background, roles, responsibilities to determine that board of directors has sufficient members who were independent from management and objective in evaluations and decision making.	No exceptions noted.

CC1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC1.3.1	The entity evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revises these when necessary to help meet changing commitments and requirements.	Obtained and inspected the organizational chart with roles and the hierarchy of high-level managers and executives, risk management policies, and the annual risk assessment performed to determine the organizational structure, reporting lines, authorities and business planning processes were evaluated.	No exceptions noted.
CC1.3.2	Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors.	Obtained and inspected evidence of the job descriptions, roles and responsibilities for key IT positions to determine that roles and responsibilities were defined in written job descriptions and communicated to managers and their supervisors.	No exceptions noted
CC1.3.3	Employees’ performance is evaluated on an annual basis.	For a sample of new hires, obtained and inspected evidence of the annual performance evaluations performed during the audit period to determine that employees’ performances were evaluated on an annual basis.	No exceptions noted.
CC1.3.4	Job requirements are documented in job descriptions and candidates' ability to meet these requirements are evaluated as part of the hiring or evaluation process.	Obtained and inspected job requirements/descriptions that are documented and available along with onboarding checklist to determine that job requirements were documented in job descriptions and candidates' ability to meet these requirements are evaluated as part of the hiring/evaluation processes.	No exceptions noted.

CC1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC1.4.1	Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process.	For a sample of new hires, obtained and inspected job requirements/descriptions that are documented and available along with onboarding checklist to determine that job requirements were documented in job descriptions and candidates' ability to meet these requirements are evaluated as part of the hiring/evaluation processes.	No exceptions noted.
CC1.4.2	Management establishes skills and continued training with its commitments and requirements for employees.	For a sample of new hires, obtained and inspected security awareness training logs and material to determine that management established skills and continued training with its commitments and requirements for employees.	No exceptions noted.
CC1.4.3	Management monitors compliance with training requirements.	Obtained and inspected evidence of ongoing monitoring for compliance by management for training requirements to determine that management monitored compliance with training requirements.	No exceptions noted.

CC1.5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC1.5.1	Roles and responsibilities are defined in written job descriptions and reviewed by management on an (as needed basis) for needed changes.	For a sample of active employees, obtained and inspected evidence of the annual performance evaluations performed during the audit period to determine annual performance reviews were conducted to review roles and responsibilities.	No exceptions noted.
CC1.5.2	The entity management and the board of directors perform annual performance evaluations to communicate and hold individuals accountable for performance of internal control responsibilities. The performance evaluation is signed by the manager and employee. Corrective actions, including training or sanctions, as necessary.	For a sample of active employees, obtained and inspected evidence of the annual performance evaluations performed during the audit period to determine management and the board of directors performed annual performance evaluations to communicate and hold individuals accountable for their performance.	No exceptions noted.

COMMUNICATION AND INFORMATION

CC2.1: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC2.1.1	System descriptions are available to customers that describe the boundaries of the systems and relevant system components.	Obtained and inspected evidence of the system descriptions availability to customers on the company intranet to determine that system descriptions were available to customers describing the boundaries of the systems and relevant system components.	No exceptions noted.
CC2.1.2	The entity performs vulnerability assessment at least quarterly to identify the required internal controls for key information systems to achieve the entity's service commitments and system requirements.	Obtained and inspected the employee handbook and completed vulnerability scans to determine that vulnerability assessments were performed at least quarterly to identify the required internal controls for key information systems.	No exceptions noted.
CC2.1.3	Detailed user and administration guides are available to external users which describe the capabilities, functions, and configuration attributes of the application.	Obtained and inspected evidence of user and administration guides availability to external users to determine that user and administration guides were available to external users describing the capabilities, functions, and configuration attributes of the application.	No exceptions noted.
CC2.1.4	Planned changes, updates and security testing schedules are communicated to internal staff through Wikis that are maintained on the internal confluence portal.	Obtained and inspected screenshot evidence of the Security Schedule and Reports document to determine that changes, updates, and security testing schedules were communicated and maintained on the internal confluence portal.	No exceptions noted.

CC2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC2.2.1	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security of the system, is provided to personnel to carry out their responsibilities.	Obtained and inspected evidence of a document that talks about designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security of the system to determine that information relevant to the security of the system were provided to personnel to carry out their responsibilities.	No exceptions noted.
CC2.2.2	Employment agreements incorporate provisions and/or terms for adherence to established information governance, and Acceptable Use policy outlines standards employees must adhere to.	For a sample of new hires, obtained and inspected signed employment agreements and acceptable use policy to determine employment agreements incorporated provisions for adherence to established information governance, and Acceptable Use policy outlines standards.	No exceptions noted.
CC2.2.3	Personnel are required to attend annual security, confidentiality, and privacy training.	For a sample of active employees, obtained and inspected evidence of completed security, confidentiality, and privacy training to determine that all personnel were required and complete annual trainings.	No exceptions noted.
CC2.2.4	Information Security Policies are available to employees on the intranet.	Obtained and inspected evidence of the Information Security Policy, and the portal showing policies are available for all employees to determine that the Information Security Policies were available to employees on the intranet.	No exceptions noted.
CC2.2.5	Information on the architecture, development, maintenance, and security of the application is available to employees on the intranet.	Obtained and inspected the portal showing information on the architecture, development, maintenance, and security are available for all employees to determine information was available to employees on the intranet.	No exceptions noted.

CC2.3: The entity communicates with external parties regarding matters affecting the functioning of internal control.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC2.3.1	System descriptions are available to customers that describe the boundaries of the systems and relevant system components.	Obtained and inspected evidence of the system descriptions availability to customers on the company intranet to determine that system descriptions were available to customers describing the boundaries of the systems and relevant system components.	No exceptions noted.
CC2.3.2	Employment agreements incorporate provisions and/or terms for adherence to established information governance, and Acceptable Use policy outlines standards employees must adhere to.	For a sample of new hires, obtained and inspected signed employment agreements and acceptable use policy to determine employment agreements incorporated provisions for adherence to established information governance, and Acceptable Use policy outlines standards.	No exceptions noted.
CC2.3.3	The entity posts a description of its system, system boundaries, and system processes that include infrastructure, software, people, processes and procedures, and data on its intranet for internal users and on the internet for external users.	Obtained and inspected evidence showing system processes for infrastructure, software, people, and procedures are available for internal and external users to determine that the entity posted descriptions of its system on the intranet for internal users and on the internet for external users.	No exceptions noted.
CC2.3.4	The entity's security commitments are communicated to external users, as appropriate.	Obtained and inspected the information security program to determine the entity's security commitments were communicated to external users.	No exceptions noted.
CC2.3.5	Subcontractors and vendors with responsibility for designing, development and/or monitoring of the application are provided information on the architecture and security requirements of the application in order for them to fulfill their responsibilities.	Obtained and inspected architecture and security requirements along with the list of applications and their appropriate owners to determine that subcontractors and vendors were provided information on the architecture and security requirements for the application in order for them to fulfill their responsibilities.	No exceptions noted.

RISK ASSESSMENT

CC3.1: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC3.1.1	Formal information sharing agreements are in place with related parties and vendors. These agreements include confidentiality commitments applicable to that entity. Agreement terms include requirements for marking and identifying data as confidential, handling standards for confidential data in the custody of related parties and vendors and return and disposal of confidential information when no longer required.	Obtained and inspected evidence showing risks are assessed and updated as needed along with the annual risk assessment performed with results provided to determine a documented risk management program was in place, and risk assessments were performed on an annual basis.	No exceptions noted.
CC3.1.2	A risk management policy governs the identification of risk and effectiveness and mitigation strategies.	Obtained and inspected risk management policy and procedures and risk Assessment worksheet showing potential threats to security and the mitigation strategies to determine that a risk management policy governs the identification of risk, effectiveness, and mitigation strategies.	No exceptions noted.

CC3.2: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC3.2.1	A master list of the entity's system components is maintained, accounting for additions and removals, for management's use.	Obtained and inspected the list of all in scope Systems and Applications with owners and criticality to determine a master list of the entity's system components were maintained for management's use.	No exceptions noted.
CC3.2.2	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Obtained and inspected risk management policies and the risk analysis/assessment worksheets to determine there was a defined formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC3.2.3	During the risk assessment and management process, risk management office personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	Obtained and inspected evidence that management identifies changes during the risk assessment and management process to determine that during the risk assessment/management process, office personnel identify changes to business objectives, commitments/requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats.	No exceptions noted.
CC3.2.4	Identified risks are rated using a risk evaluation process and ratings are reviewed by management.	Obtained and inspected the risk evaluation process and the ratings were reviewed by management as part of the ongoing risk management process to determine that Identified risks were rated using a risk evaluation process and ratings were reviewed by management.	No exceptions noted.
CC3.2.5	The risk and controls group evaluate the effectiveness of controls and mitigation strategies in meeting identified risks annually and recommends changes based on its evaluation.	Obtained and inspected of risks were rated using an evaluation process to determine the risk and controls group evaluates the effectiveness of controls and mitigation strategies in meeting identified risks and recommendations were made.	No exceptions noted.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC3.2.6	The risk and controls group's recommendations are reviewed and approved by senior management.	Obtained and inspected the risk evaluation process and the ratings were reviewed by management as part of the ongoing risk management process to determine the risk and control group's recommendations were reviewed and approved by senior management.	No exceptions noted.

CC3.3: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC3.3.1	Potential fraud risks are included in the risk evaluation process and are rated by management.	Through inquiry and observation with management, determined that monitoring tools were in place to identify and evaluate ongoing, security threats, fraud detection and monitoring systems, and incident tracking systems. Obtained and inspected the risk evaluation process and completed risk assessment reviewed by management to determine identified risks, including potential fraud risks are rated using a risk evaluation process and ratings are reviewed by management.	No exceptions noted.
CC3.3.2	Management uses information technology tools such as security systems, fraud detection and monitoring systems, and incident tracking systems to identify and manage fraud risk.	Through inquiry and observation with management, determined that monitoring tools were in place to identify and evaluate ongoing, security threats, fraud detection and monitoring systems, and incident tracking systems. Obtained and inspected screenshot evidence of the monitoring dashboards to determine that security, access fraud, and incident tracking were in place.	No exceptions noted.
CC3.3.3	The entity has established measures to protect against unauthorized and willful acquisition, use, or disposal of assets.	Obtained and inspected the employee handbook to determine there were established measures to protect against unauthorized and willful acquisition, use, or disposal of assets.	No exceptions noted.

CC3.4: The entity identifies and assesses changes that could significantly impact the system of internal control.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC3.4.1	Ongoing internal and external vulnerability scans are performed to maintain the on-going security posture of the application.	Obtained and inspected internal and external vulnerability scan reports to determine ongoing internal and external vulnerability scans were performed to maintain the on-going security posture of the application.	No exceptions noted.

MONITORING ACTIVITIES

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.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC4.1.1	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. This software sends a message to the operations center. Incident, problem, or change management "tickets" are recorded when specific predefined thresholds are met.	Through inquiry and observation with management, determined that monitoring tools were in place to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. Obtained and inspected screenshot evidence of the Cyrebro and Azure monitoring dashboards and alert tickets to determine that configurations were in place to actively monitor and send email alerts to the teams. Obtained and inspected screenshot evidence of the customer incident dashboard to determine that the customer support team actively monitored and tracked tickets for client related issues.	No exceptions noted.
CC4.1.2	Operations and security personnel follow defined protocols for resolving and escalating reported events.	Through inquiry and observation with management, determined that a standard procedure for evaluating incidents was in place, including documenting an RCA for incidents that require it. For a sample of critical incidents, obtained and inspected the RCA document to determine that an analysis had been performed and a plan of action was included to address future changes .	No exceptions noted.
CC4.1.3	Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments.	Obtained and inspected copies of managements ongoing evaluations to determine management used a variety of different types of ongoing and separate evaluations, including penetration testing.	No exceptions noted.

CC4.2: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC4.2.1	Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.	Obtained and inspected scan report results to determine that scans were completed, and deficiencies were communicated to parties requiring corrective action.	No exceptions noted.
CC4.2.2	The entity has established a practice that requires all deficiencies rated as serious threats to be reported to senior management.	Obtained and inspected scan report results to determine that scans were completed, and deficiencies rated as serious were required to be reported to senior management.	No exceptions noted.

CONTROL ACTIVITIES

CC5.1: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC5.1.1	The risk and controls group evaluate the effectiveness of controls and mitigation strategies in meeting identified risks annually and recommends changes based on its evaluation.	Obtained and inspected of risks were rated using an evaluation process to determine the risk and controls group evaluates the effectiveness of controls and mitigation strategies in meeting identified risks and recommendations were made.	No exceptions noted.
CC5.1.2	For business continuity purposes, the disaster recovery plans are tested annually.	Obtained and inspected copies of BCP and DRP test results to determine that for business continuity purposes, the disaster recovery plans were tested annually.	No exceptions noted.
CC5.1.3	Penetration test scans are done annually, and their frequency is adjusted as required to meet ongoing and changing commitments and requirements.	Obtained and inspected the latest vulnerability scan reports for internal and external scans and re-run reports showing any vulnerabilities are identified and remediated to determine that annual penetration tests were completed, and any vulnerabilities identified were remediated.	No exceptions noted.
CC5.1.4	The organization establishes information security objectives at relevant functions and levels.	Obtained and inspected evidence of the information security policies to determine that the organization established information security objectives at relevant functions and levels.	No exceptions noted.

CC5.2: The entity also selects and develops general control activities over technology to support the achievement of objectives.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC5.2.1	As part of the IT planning and management, risks affecting IT projects and recommended courses of action are identified, tracked, and discussed.	Obtained and inspected evidence that management identifies changes during the risk assessment and management process to determine that during the risk assessment/management process, office personnel identify changes to business objectives, commitments/requirements, internal operations, and external factors that threaten the achievement of business objectives and updated the potential threats.	No exceptions noted.
CC5.2.2	Management develops a list of control activities to mitigate the security risks identified during the annual risk assessment process.	Obtained and inspected control activities that mitigate the security risks identified to determine that management develops a list of control activities to mitigate the security risks identified during the annual risk assessment processes.	No exceptions noted.

CC5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC5.3.1	Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.	Obtained and inspected the policies and procedures established by management including the acceptable use policy, access control standards, and application network security standards to determine that policy reviews and changes were updated, as necessary.	No exceptions noted.
CC5.3.2	The entity's Security Governance Committee is charged with establishing and maintaining the overall security policies and procedures.	Obtained and inspected HR Acuity's information security governance plan to determine the Security Governance Committee was charged with establishing and maintaining the overall security policies and procedures.	No exceptions noted.
CC5.3.3	The entity has assigned personnel responsible for establishing, maintaining, and enforcing the overall security policies and procedures.	Obtained and inspected personnel who are assigned for maintaining and enforcing the overall security policies and procedures to determine there were assigned personnel responsible for establishing, maintaining, and enforcing the overall security policies and procedures.	No exceptions noted
CC5.3.4	The entity's policy and procedure manuals are reviewed annually by management for consistency with the organization's risk mitigation strategy and updated as necessary for changes in the strategy. Human resources personnel screen internal and external job applicant qualifications based on the defined requirements within the job description. Transcripts are obtained to evidence educational attainment, and job references are checked to validate experience.	Through inquiry and observation with the HR Manager, determined that job applicants were required to submit resumes and answer questions based on job role through the HR tool. Obtained and inspected evidence of job descriptions and hiring process workflow documents to determine that candidate qualifications were assessed prior to onboarding. Obtained and inspected policies and procedures to determine that manuals and workflows were updated and reviewed annually.	No exceptions noted.

Control No.	***Control Activity***	***Test of Operating Effectiveness***	***Conclusion***
CC5.3.5	The entity's policy and procedure manuals are reviewed annually by management for consistency with the organization's risk mitigation strategy and updated as necessary for changes in the strategy.	Obtained and inspected evidence of management conducting annual reviews of the policies and procedures to determine that policy and procedure manuals were reviewed annually by management.	No exceptions noted.

Supplemental Criteria: 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.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC6.1.1	Established entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists.	Obtained and inspected the Infrastructure and Software Hardening Standards and Password Policies to determine the entity standards exist for infrastructure, software hardening and configuration.	No exceptions noted.
CC6.1.2	Network scans are performed for infrastructure elements to identify variance from entity standards.	Obtained and inspected the latest vulnerability scan reports for internal and external scans and re-run reports showing any vulnerabilities are identified and remediated to determine annual network scans were completed and vulnerabilities were identified and remediated.	No exceptions noted.
CC6.1.3	Assets are assigned owners who are responsible for evaluating access based on job roles. The owners define access rights when assets are acquired or changed and periodically evaluate access for assets under their custody or stewardship.	Obtained and inspected a list of all systems and their responsible owners to determine that assets are assigned to owners that were responsible for evaluating access based on job roles.	No exceptions noted.
CC6.1.4	Infrastructure components and software are configured to use the single sign-on functionality when available. Systems not using the single sign- on functionality are required to be implemented with separate user ID and password submission.	Obtained and inspected evidence of configurations using the single sign-on, systems that do not use single sign-on authentication, and Active Directory settings to determine that infrastructure components and software were configured to use the single sign-on functionality.	No exceptions noted.
CC6.1.5	External access by employees is permitted only through a two factor (for example, a swipe card and a password) encrypted virtual private network (VPN) connection.	Obtained and inspected the network diagram to determine that access points by employees were documented. Through inquiry and observation with management, determined that VPN and MFA were enabled to help ensure only valid users gain access to IT components. Obtained and inspected screenshot evidence of remote login utilizing VPN and MFA to determine that specific IT components were configured for VPN and MFA.	No exceptions noted.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC6.1.6	A role-based security process has been defined with an access control system that is required to use roles when possible.	Obtained and inspected the applications and ownership document to determine role-based security processes were defined with an access control system that was required to use roles when possible.	No exceptions noted.
CC6.1.7	Privileged access to sensitive resources is restricted to defined user roles and access to these roles must be approved by the chief information security officer. This access is reviewed by the chief information security officer on a periodic basis as established by the chief information security officer.	Obtained and inspected the applications and ownership document and a list of administrative roles to determine privileged access to sensitive resources was restricted to defined user roles.	No exceptions noted.
CC6.1.8	The online application matches each user ID to a single customer account number. Requests for access to system records require the matching of the customer account number.	Obtained and inspected evidence of online application user IDs to determine online applications matched each user ID to a single customer account number and requests for access to system records required the matching of the customer account number.	No exceptions noted.
CC6.1.9	Two factor authentication and use of encrypted VPN channels help to ensure that only valid users gain access to IT components.	Through inquiry and observation with management, determined that VPN and MFA were enabled to help ensure only valid users gain access to IT components. Obtained and inspected screenshot evidence of remote login utilizing VPN and MFA to determine that specific IT components were configured for VPN and MFA.	No exceptions noted.
CC6.1.10	Users can only access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system.	Through inquiry and observation with management, determined that VPN and MFA were enabled to help ensure only valid users gain access to IT components. Obtained and inspected screenshot evidence of remote login utilizing VPN and MFA to determine that specific IT components were configured for VPN and MFA. Obtained and inspected screenshot evidence of the SSL certificate to determine that secure connection access was in place.	No exceptions noted.

Control No.	Control Activity	Test of Operating Effectiveness	Conclusion
CC6.1.11	Password complexity standards are established to enforce control over access control software passwords.	Obtained and inspected evidence of password policy and procedures and evidence that password complexity requirements are enforced to determine password complexity standards were established to enforce control over access control software passwords.	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.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC6.2.1	Employee access to protected resources is created or modified by the authorized group based on an authorized change request from the system's asset owner.	For a sample of new hires, obtained and inspected onboarding/offboarding checklist and evidence of new hires gaining access to determine employee access to protected resources was created or modified by the authorized group based on an authorized change request from the system's asset owner.	No exceptions noted.
CC6.2.2	Processes are in place to remove credential access when an individual no longer requires such access.	For a sample of terminated employees, obtained and inspected evidence of online and physical access being revoked along with offboarding tickets and checklists to determine that processes were in place to remove credential access when an individual no longer requires such access.	No exceptions noted.

CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC6.3.1	When possible, formal role-based access controls that limit access to system and infrastructure components are created, and these are enforced by the access control system.	Obtained and inspected the network diagram, the applications and ownership document, and a list of administrative roles to determine that formal role-based access controls for limited access to system and infrastructure components were created.	No exceptions noted.
CC6.3.2	User access requests for a specific role are approved by the user manager or designated approver via the change management system.	For a sample of new hires, obtained and inspected the process for access granted to new hires along with onboarding and off-boarding procedures to determine user access requests for specific roles were approved by the user manager or designated approver via the change management system.	No exceptions noted.
CC6.3.3	Roles are reviewed and updated by asset owners and the risk and controls group on an annual basis. Access change requests resulting from the review are submitted to the security group via a change request record.	Obtained and inspected the applications and ownership document and system access permissions to determine that roles were reviewed and updated by asset owners and the risks and control groups on an annual basis.	No exceptions noted.

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC6.4.1	An ID card-based physical access control system has been implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.	Through inquiry and observation with management, the ID card-based physical access of control system to determine front and back door had ID card-based access and an access log was kept.	No exceptions noted.
CC6.4.2	The Human Resources department notifies the appropriate administrators when an employee or contractor is terminated. Requests to remove physical access are documented in the ticketing system, and access is promptly revoked.	For a sample of terminated employees, obtained and inspected evidence of physical access to facilities and protected information assets was revoked for terminated employees to determine that requests to remove physical access was documented, and access was promptly revoked.	No exceptions noted.
CC6.4.3	Management periodically reviews access rights on an as needed basis based on personnel changes to verify that access privileges are in accordance with approved access and job responsibilities. Inappropriate access, if any, is promptly removed.	Obtained and inspected evidence of physical access review performed to determine management reviewed access rights on an as-needed basis and inappropriate access was promptly removed.	No exceptions noted.

CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC6.5.1	Formal data retention and disposal procedures are in place to guide the secure disposal of the company's and customers' data.	Obtained and inspected evidence of the policies and procedures regarding the retention and disposal of data to determine formal data retention and disposal procedures were in place to guide the secure disposal of the company's and customers' data.	No exceptions noted.
CC6.5.2	Prior to removal from company facilities, all digital media is completely degaussed and sanitized to remove any data and software.	Obtained and inspected evidence of the data privacy policy to determine there were policies in place for all digital media to be completely degaussed and sanitized to remove any data and software.	No exceptions noted.

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC6.6.1	Defined entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists that define which privileges are attributable to each user or system account.	Obtained and inspected network diagrams for access to the network, showing no external access was permitted into the managed network to determine entity standards exist for infrastructure and software hardening and configurations.	No exceptions noted.
CC6.6.2	External points of connectivity are protected by a firewall complexity.	Obtained and inspected network diagrams for access to the network, showing no external access was permitted into the managed network to determine external points of connectivity are protected by a firewall complexity.	No exceptions noted.
CC6.6.3	Firewall hardening standards are based on relevant applicable technical specifications, and these are compared against product and industry recommended practices and updated periodically.	Obtained and inspected the Infrastructure and Software Hardening Standards and Password Policies to determine firewall hardening standards were based on relevant applicable technical specifications and industry recommended practices.	No exceptions noted.
CC6.6.4	External access to nonpublic sites is restricted through the use of user authentication such as VPN.	Through inquiry and observation with management, determined that VPN and MFA were enabled to help ensure only valid users gain access to IT components. Obtained and inspected screenshot evidence of remote login utilizing VPN and MFA to determine that external access to nonpublic sites was restricted through VPN.	No exceptions noted.
CC6.6.5	The types of activities that can be performed from external connection are restricted and the corporate VPN is required to access all permitted systems.	Through inquiry and observation with management, determined that VPN and MFA were enabled to help ensure only valid users gain access to IT components. Obtained and inspected screenshot evidence of remote login utilizing VPN and MFA to determine that VPN was required to access all permitted systems.	No exceptions noted.

CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC6.7.1	VPN, SSL, and other encryption technologies are used for defined points of connectivity and to protect communications between the processing center and users connecting to the processing center from within or external to customer networks.	Through inquiry and observation with management, determined that VPN and MFA were enabled to help ensure only valid users gain access to IT components. Obtained and inspected screenshot evidence of remote login utilizing VPN and MFA to determine that specific IT components were configured for VPN and MFA. Obtained and inspected screenshot evidence of the SSL certificate to determine that secure connection access was in place.	No exceptions noted.
CC6.7.2	Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths (for example, e-mail) unless it is encrypted.	Obtained and inspected evidence of the Computer and Network Security Policy to determine entity policies prohibited the transmission of sensitive information over the Internet or other public communications.	No exceptions noted.
CC6.7.3	Storage for workstations and laptops is encrypted. Copying sensitive data into removable media is monitored.	For a sample of workstations and laptops, obtained and inspected the EDR report to determine that device storage was encrypted, and removable media was being monitored.	Exception noted. For 1 of the 8 laptops selected, no evidence of encryption was provided.

Management Response to Exception Noted in CC6.7.3

Encryption did not take during the initial setup of the laptop. There is a SOP with a checklist for workstation deployments. A new task has been added to validate encryption by checking the Operation System information and cloud management console. In addition, a full reconciliation of systems will be performed quarterly to ensure encryption is enforced.

<u>CC6.8:</u> The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC6.8.1	The ability to install software on workstations and laptops is restricted to specific roles only.	Obtained and inspected evidence of AD groups to show list of users with access roles to install software to determine the ability to install software on workstations and laptops was restricted to specific roles only.	No exceptions noted.
CC6.8.2	Antivirus software is installed on workstations, laptops, and servers supporting such software.	For a sample of endpoints, obtained and inspected screenshot evidence to determine that antivirus was installed and configured appropriately.	No exceptions noted.
CC6.8.3	Antivirus software is configured to receive an updated virus signature at least daily. Designated teams review reports of devices that have not been updated in 30 days and follows up on the devices.	Obtained and inspected screenshot evidence of the antivirus configuration to determine that signature updates were configured to update daily. Obtained and inspected a monthly asset report to determine that a review of devices was performed including assets that were out of compliance.	No exceptions noted.

Supplemental Criteria: 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.

.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC7.1.1	An IT infrastructure monitoring tool is utilized to monitor IT infrastructure availability and performance and generates alerts when specific predefined thresholds are met.	Through inquiry and observation with management, determined that monitoring tools were in place to identify and evaluate ongoing system performance and infrastructure availability. Obtained and inspected screenshot evidence of the Azure monitoring dashboards and alert tickets to determine that configurations were in place to actively monitor and send email alerts to the teams when predefined thresholds were met.	No exceptions noted.
CC7.1.2	The entity utilizes a configuration monitoring tool that monitors and verifies changes to production systems configurations.	Through inquiry and observation with management, determined that monitoring tools were in place to monitor and verify changes to production systems configurations. Obtained and inspected screenshot evidence of the monitoring dashboard and alert tickets to determine that configurations were in place to actively monitor and send email alerts to the teams when predefined thresholds changes were made.	No exceptions noted.
CC7.1.3	Internal and external network vulnerability scans are performed quarterly. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Obtained and inspected quarterly vulnerability scan reports and remediation plans for high and critical vulnerabilities to determine that internal and external network vulnerability scans were performed quarterly and remediation plans for high vulnerabilities were implemented.	No exceptions noted.

<u>CC7.2:</u> 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.

Control No.	***Control Activity***	***Test of Operating Effectiveness***	***Conclusion***
CC7.2.1	Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity or service requests. This software sends a message to the operations center and security organization and automatically opens a priority incident or problem ticket.	Through inquiry and observation with management, determined that monitoring tools were in place to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. Obtained and inspected screenshot evidence of the Cyrebro and Azure monitoring dashboards and alert tickets to determine that configurations were in place to actively monitor and send email alerts to the teams. Obtained and inspected screenshot evidence of the monthly asset and endpoint report to determine that logging and monitoring endpoint data was performed.	No exceptions noted.
CC7.2.2	The entity utilizes an external SOC monitoring service to continuously review the systems to detect anomalous activity or changes to the baseline configuration.	Obtained and inspected evidence of external monitoring service is used to continuously review the system to determine the entity utilized an external monitoring service to continuously review the systems to detect anomalous activity or changes to the baseline configuration.	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.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC7.3.1	Operations personnel follow defined protocols for evaluating resolving and escalating reported events. Security related events are assigned to the security group for evaluation.	Through inquiry and observation with management, determined that a standard procedure for evaluating incidents was in place, including documenting an RCA for incidents that require it. For a sample of critical incidents, obtained and inspected the RCA document to determine that an analysis had been performed and a plan of action was included to address future changes.	No exceptions noted.
CC7.3.2	Customer impacting incidents are communicated to the relevant customers in a timely manner.	Obtained and inspected evidence of customer impacting incidents communication to customers to determine customer impacting incidents were communicated to the relevant customers and all incidents were logged and tracked to completion.	No exceptions noted.
CC7.3.3	The resolution of high severity incidents and the overall incident status is reviewed at the weekly operations and relevant stakeholders group meetings.	Through inquiry and observation with management, determined that a twice weekly meeting occurs to review issues and incidents, including all high severity incidents. For a sample of weeks, obtained and inspected the CLIMP Board meeting recurring meeting invite to determine that incident statuses were reviewed on a weekly basis.	No exceptions noted.
CC7.3.4	Entity policies include probation, suspension, and termination as potential sanctions for employee misconduct.	Obtained and inspected evidence of termination policy to determine the entity has policies include counseling, verbal warning, written warning, final written warning, and termination for employee misconduct.	No exceptions noted.

CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC7.4.1	Management has established defined roles and responsibilities to oversee implementation of information security policies including incident response.	Obtained and inspected policies and procedures related to information security, including incident response, to determine defined roles and responsibilities for implementation and enforcement were documented in the policies.	No exceptions noted.
CC7.4.2	All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	Obtained and inspected evidence of the incident response plan in place, and remediation plans to determine incidents related to the security of the system were logged, tracked, and communicated to affected parties by management until resolved.	No exceptions noted.
CC7.4.3	Backups are configured for the databases to run on a daily basis and are retained for 30 days.	Obtained and inspected the Backup policy to determine that procedures were in place for database backups. Obtained and inspected screenshot evidence of the backup configurations and schedule to determine that backups ran on a daily basis and retention was set to 30 days.	No exceptions noted.
CC7.4.4	Internal and external network vulnerability scans are performed quarterly. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Obtained and inspected quarterly vulnerability scan reports and remediation plans for high and critical vulnerabilities to determine that internal and external network vulnerability scans were performed quarterly and remediation plans for high vulnerabilities were implemented.	No exceptions noted.

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC7.5.1	An administrator responsible for security incident tickets follows a process of analyzing the security incident. The process begins with detailing what specific attack occurred, which system(s) were affected and what happened during the attack. Next the root cause is determined, and the event is given a classification to assign the level of impact of the event. The impact level is based on guidelines detailed in the procedures.	Through inquiry and observation with management, determined that a twice weekly meeting occurs to review issues and incidents, including all high severity incidents. For a sample of weeks, obtained and inspected the CLIMP Board meeting recurring meeting invite to determine that incident statuses were reviewed on a weekly basis.	No exceptions noted.
CC7.5.2	Annual testing of the incident response plan is performed using tabletop exercises and simulations to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned from tabletop exercises are used to implement changes to reflect effective procedures when handling incidents.	Obtained and inspected evidence of BCP and DRP test results and the annual incident response plan tabletop exercise results to determine annual testing of the incident response plan is performed using tabletop exercises and simulations to ensure the incident response procedures are up-to-date and accurate.	No exceptions noted.

Supplemental Criteria: 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.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC8.1.1	During the ongoing risk assessment process and the periodic planning, the infrastructure, data, software, and procedures are evaluated for needed changes. Change requests are created based on the identified needs.	Obtained and inspected evidence of the risk assessment and change management policies and procedures to determine during the ongoing risk assessment process procedures are evaluated for needed changes and change requests are created based on the identified needs.	No exceptions noted.
CC8.1.2	For high severity incidents, a root cause analysis is prepared and reviewed by operations management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution.	Through inquiry and observation with management, determined that a standard procedure for evaluating incidents was in place, including documenting an RCA for incidents that require it. For a sample of critical incidents, obtained and inspected the RCA document to determine that an analysis had been performed and a plan of action was included to address future changes.	No exceptions noted.
CC8.1.3	Controls are in place to ensure that systems software latest required versions, patches and releases are identified and assessed on a regular/continuous basis. Intentional exceptions (patch not applied for a reason) are documented and approved by management.	Obtained and inspected evidence of secure software development policies, meeting notes discussing updates, and an example from Visual Studios software update to determine policies were in place to ensure that systems software latest required versions, patches and releases were identified and assessed on a regular/continuous basis.	No exceptions noted.
CC8.1.4	Controls are in place to ensure that system software updates required by the Company are evaluated and tested prior to implementation in the production environment.	Obtained and inspected evidence of secure software development policies, and an example from Visual Studios software update to determine controls were in place to ensure that system software updates were evaluated and tested prior to implementation into production.	No exceptions noted.
CC8.1.5	Application changes require the approval of the designated approver prior to implementation into production.	For a sample of sprints and application changes, obtained and inspected ticket evidence to determine that changes received appropriate approval prior to implementation into production.	No exceptions noted.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC8.1.6	Test plans and test data are created and used in required system testing.	For a sample of sprints and application changes, obtained and inspected ticket evidence to determine that changes were tested with test data in non-production environments prior to implementation into production.	No exceptions noted.
CC8.1.7	Established entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists.	Obtained and inspected the Infrastructure and Software Hardening Standards and Password Policies to determine the entity standards exist for infrastructure, software hardening and configuration.	No exceptions noted.
CC8.1.8	Separate environments are used for development, testing, and production. Developers do not have the ability to make changes to software in production.	Obtained and inspected the network diagram, and a permissions access log to determine separated environments are used for development, testing, and production.	No exceptions noted.
CC8.1.9	Post implementation procedures that include verification of operations are performed after the implementation of impactful changes and a rollback plan is defined.	Obtained and inspected evidence of software updates that occurred during the audit period and post implementation procedures to determine after implementation, procedures including verification of operations are performed after the implementation of impactful changes and a rollback plan was defined.	No exceptions noted.
CC8.1.10	The change management process has defined the following roles and assignments.	Obtained and inspected evidence of segregation of duties and roles are properly assigned to determine change management processes have defined roles and assignments.	No exceptions noted.

Supplemental Criteria: Risk Mitigation

CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC9.1.1	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed.	Obtained and inspected evidence showing risks are assessed and updated as needed along with the annual risk assessment performed with results provided to determine a documented risk management program was in place, and risk assessments were performed on an annual basis.	No exceptions noted.

CC9.2: The entity assesses and manages risks associated with vendors and business partners.

Control No.	*Control Activity*	*Test of Operating Effectiveness*	*Conclusion*
CC9.2.1	Formal information sharing agreements are in place with related parties and vendors. These agreements include confidentiality commitments applicable to that entity. Agreement terms include requirements for marking and identifying data as confidential, handling standards for confidential data in the custody of related parties and vendors and return and disposal of confidential information when no longer required.	For a sample of third parties and vendors, obtained and inspected agreement commitments to determine that agreements included confidentiality commitments, including data handling of sensitive or confidential data.	No exceptions noted.
CC9.2.2	Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available. Assessment procedures are performed based on the entity's vendor management criteria.	For a sample of third parties and vendors, obtained and inspected the compliance report packets to determine that vendor risk assessment procedures, including obtaining and reviewing attestation reports, was performed.	No exceptions noted.
CC9.2.3	Vendor NDA's and contracts contain language attesting to confidentiality agreements.	For a sample of third parties and vendors, obtained and inspected agreement commitments to determine that agreements included confidentiality commitments, including data handling of sensitive or confidential data.	No exceptions noted.

VIII. ADDITIONAL INFORMATION PROVIDED BY THE INDEPENDENT SERVICE AUDITOR

Selection Criteria for Specific Tests

In selecting tests of the operating effectiveness of controls, we considered the

a) nature of the items being tested,
b) the types and adequacy of available evidential matter,
c) the nature of the trust services criteria to be achieved, and
d) the expected efficiency and effectiveness of the test.

Types and Descriptions of the Tests of Operating Effectiveness

Various testing methods are used to assess the operating effectiveness of controls during the examination period. The table below describes the various methods that were employed in testing the operating effectiveness of controls that are in place at the Company.

Testing Procedure	Description
Inquiry	Inquired of appropriate personnel and corroborated with management.
Observation	Observed the application or existence of the specific control as represented.
Inspection	Inspected documents and records indicating performance of the control.
Reperformance	Reperformed the control, or processing of the application control, for accuracy of its operation.

Procedures for Assessing Completeness and Accuracy of Client-Provided Information (“CPI”)

For tests of controls requiring the use of CPI (for example, controls requiring system-generated populations for sample-based testing), we performed a combination of the following procedures where possible, based on the nature of the CPI, to address the completeness, accuracy, and integrity of the data or reports used:

a) inspect the source of the CPI,
b) inspect the query, script, or parameters used to generate the CPI,
c) tie data between the CPI and the source, and/or
d) inspect the CPI for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

In addition to the above procedures, for tests of controls requiring management’s use of CPI in the execution of the controls (for example, periodic reviews of user access listings), we inspected management’s procedures to assess the validity of the CPI source and the completeness, accuracy, and integrity of the data or reports.