Process Automation Platform

SOC 2® Type 2 – Reporting on Controls at a Service Organization

Security with Trust Services Criteria for Security mapped to ISO 27001 Requirements

November 1, 2022 to October 31, 2023

With Independent Service Auditor's Report by Barnes Dennig

InfoReady
Process Automation Platform
SOC 2® Type 2 – Reporting on Controls at a Service Organization
Trust Services Criteria for Security Mapped to ISO 27001 Requirements
November 1, 2022 to October 31, 2023

Table of Contents

Section I – Assertion of the Management of InfoReady 3

Section II – Independent Service Auditor's Report 6

Section III – Description of InfoReady's Process Automation Platform 11

Section IV – Trust Services Criteria Relevant to Security, Trust Services Criteria for Security Mapped to ISO 27001 Requirements, Related Controls and Tests of Controls 27

Section I – Assertion of the Management of InfoReady

Assertion of the Management of InfoReady

We have prepared the accompanying description of InfoReady's Process Automation Platform system titled "Description of InfoReady's Process Automation Platform" throughout the period November 1, 2022 to October 31, 2023 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria,* (description criteria). The description is intended to provide report users with information about the Process Automation Platform system that may be useful when assessing the risks arising from interactions with InfoReady's system, particularly information about system controls that InfoReady 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 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria* and the applicable trust services criteria mapped to the corresponding ISO 27001 requirements.

InfoReady uses subservice organizations for the following services:

Subservice Organization	Services Provided
Amazon Web Services (AWS)	Hosting and Infrastructure-as-a-Service
Freshdesk	External ticketing system
GDI Infotech, Inc.	Professional Employer Organization providing human resources coordination and support
Microsoft	Email, calendar and administration
Rackspace	Hosting and Infrastructure-as-a-Service
Veracode	Application security testing

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at InfoReady, to achieve InfoReady's service commitments and system requirements based on the applicable trust services criteria and the applicable trust services criteria mapped to the corresponding ISO 27001 requirements. The description presents InfoReady's controls, the applicable trust services criteria, the applicable trust services criteria mapped to the corresponding ISO 27001 requirements and the types of complementary subservice organization controls assumed in the design of InfoReady's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at InfoReady, to achieve InfoReady's service commitments and system requirements based on the applicable trust services criteria and the applicable trust services criteria mapped to the corresponding ISO 27001 requirements. The description presents the service organization's controls, the applicable trust services criteria, the applicable trust services criteria mapped to the corresponding ISO 27001 requirements and the complementary user entity controls assumed in the design of the service organization's controls.

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

1) The description presents InfoReady's Process Automation Platform system that was designed and implemented throughout the period of November 1, 2022 to October 31, 2023 in accordance with the description criteria.

2) The controls stated in the description were suitably designed throughout the period of November 1, 2022 to October 31, 2023 to provide reasonable assurance that InfoReady's service commitments and system requirements would be achieved based on the applicable trust services criteria and the applicable trust services criteria mapped to the corresponding ISO 27001 requirements, if its controls operated effectively as of that date and if the subservice organizations and user entities applied the complementary controls assumed in the design of InfoReady's controls throughout that period.

3) The controls stated in the description operated effectively throughout the period of November 1, 2022 to October 31, 2023 to provide reasonable assurance that InfoReady's service commitments and system requirements were achieved based on the applicable trust services criteria and the applicable trust services criteria mapped to the corresponding ISO 27001 requirements, if complementary subservice organization controls and complementary user entity controls assumed in the design of InfoReady's controls operated effectively throughout that period.

Maurice Collins, COO
January 16, 2024

Section II – Independent Service Auditor's Report

BARNES DENNIG
Accounting • Tax • Business Insight

OHIO
CINCINNATI OFFICE
150 E. 4th Street
Cincinnati, OH 45202
Main: 513.241.8313
Fax: 513.241.8303

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security

To: InfoReady

Scope

We have examined InfoReady's accompanying description of its Process Automation Platform system found in Section III titled "Description of InfoReady's Process Automation Platform" throughout the period November 1, 2022 to October 31, 2023 (description) based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a *SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA*, Description Criteria,* (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that InfoReady's service commitments and system requirements would be achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria* and the applicable trust services criteria for security mapped to the corresponding ISO 27001 requirements as outlined in Section IV.

InfoReady uses subservice organizations for the following services:

Subservice Organization	Services Provided
Amazon Web Services (AWS)	Hosting and Infrastructure-as-a-Service
Freshdesk	External ticketing system
GDI Infotech, Inc.	Professional Employer Organization providing human resources coordination and support
Microsoft	Email, calendar and administration
Rackspace	Hosting and Infrastructure-as-a-Service
Veracode	Application security testing

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at InfoReady, to achieve InfoReady's service commitments and system requirements based on the applicable trust services criteria and the applicable trust services criteria mapped to the corresponding ISO 27001 requirements. The description presents InfoReady's controls, the applicable trust services criteria, the applicable trust services criteria mapped to the corresponding ISO 27001 requirements and the types of complementary subservice organization controls assumed in the design of InfoReady'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 certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at InfoReady, to achieve InfoReady's service commitments and system requirements based on the applicable trust services criteria and the applicable trust services criteria mapped to the corresponding ISO 27001 requirements. The description presents

InfoReady's controls, the applicable trust services criteria, the applicable trust services criteria mapped to the corresponding ISO 27001 requirements and the complementary user entity controls assumed in the design of InfoReady'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

InfoReady is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that InfoReady's service commitments and system requirements would be achieved. In Section I, InfoReady has provided the accompanying assertion titled "Assertion of the Management of InfoReady" (assertion) about the description and the suitability of design of controls and operating effectiveness stated therein. InfoReady 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, the applicable trust services criteria mapped to the corresponding ISO 27001 requirements and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria and the applicable trust services criteria mapped to the corresponding ISO 27001 requirements. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

- 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 and the applicable trust services criteria mapped to the corresponding ISO 27001 requirements.

- 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 and the applicable trust services criteria mapped to the corresponding ISO 27001 requirements.
- evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in 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 and the applicable trust services criteria mapped to the corresponding ISO 27001 requirements. Also, the projection to the future of any conclusions about the suitability of the design or 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 listed in Section IV, "Trust Services Criteria Relevant to Relevant to Security, Trust Services criteria for Security mapped to ISO 27001 Requirements, Related Controls and Tests of Controls" of this report.

Opinion

In our opinion, in all material respects—

a) the description presents InfoReady's Process Automation Platform that was designed and implemented throughout the period of November 1, 2022 to October 31, 2023 in accordance with the description criteria.

b) the controls stated in the description were suitably designed throughout the period of November 1, 2022 to October 31, 2023 to provide reasonable assurance that InfoReady's service's commitments and system requirements would be achieved based on the applicable trust services criteria, the applicable trust services criteria mapped to the corresponding ISO 27001 requirements, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of InfoReady's controls throughout that period.

c) the controls stated in the description operated effectively throughout the period of November 1, 2022 to October 31, 2023 to provide reasonable assurance that InfoReady's service commitments and system requirements were achieved based on the applicable trust services criteria, the applicable trust services criteria mapped to the corresponding ISO 27001 requirements, if complementary subservice organization controls and complementary user entity controls assumed in the design of InfoReady's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of InfoReady; user entities of InfoReady's Process Automation Platform during some or all of the period of November 1, 2022 to October 31, 2023; business partners of InfoReady subject to risks arising from interactions with the Process Automation Platform 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 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 and the applicable trust services criteria mapped to the corresponding ISO 27001 requirements.
- 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.

Barnes Dennig & Co., Ltd.
Cincinnati, OH
January 16, 2024

Section III – Description of InfoReady's Process Automation Platform

Company Overview

InfoReady, founded in 2010, is a provider of software for research organizations, making internal grants and other application and review processes easier to manage.

Services Provided

The InfoReady Process Automation Platform is used by over 230 research organizations worldwide for managing internal grants, competitions and approval processes.

The InfoReady Process Automation Platform provides a means for administrators to promote, solicit, review/assess, select and track progress. Furthermore, it provides a means for efficient oversight and memorialization of decisions being made and executed. Working together with other institutional systems, it provides the means for all stakeholders of an organization to know exactly what they need to know when they need to know in a single place.

The Process Automation Platform comprises the subsequent applications:

- InfoReady Review™ ("Review") provides an application for form-building, routing, decision-making and reporting through user-friendly workflow tools.
- InfoReady Scale provides an application to centralize and promote program offerings.

In May 2023, Review was migrated from Rackspace to AWS. The features of Scale have been incorporated into Review. Scale continues to be hosted at Rackspace and is in the process of being sunset.

Service Commitments and System Requirements

InfoReady designs its processes and procedures to meet its objectives for its Process Automation Platform. Those objectives are based on the service commitments that InfoReady makes to user entities, the laws and regulations that govern the provision of the Process Automation Platform, and the financial, operational, and compliance requirements that InfoReady has established for the services.

InfoReady establishes operational requirements that support the achievement of security commitments, relevant laws and regulations and other system requirements. Such requirements are communicated in InfoReady'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 Process Automation Platform. The policies and procedures are based on applicable Trust Services Criteria for Security.

Security commitments include:

Credential Management
- Any passwords are stored locally using a one-way salted hash
- Local marshaling of credentials of Single Sign On (SSO support)
- SSO support includes InCommon, Shibboleth, LDAP, etc.

Service Model
- Software-As-A-Service
- Multi-tenant, Single instance implementation

• All data logically separated

Infrastructure

• Java, JavaScript, MySQL, Linux, Apache, WildFly infrastructure

Hosting

• Hosted within borders at Amazon Web Services (AWS)
• AWS protection and monitoring services deployed
• Scale, in the process of being sunset, is hosted at Rackspace

Security

• Veracode for manual and automated vulnerability scanning
• AES 256-bit encryption of data
• 128-bit SSL certificates
• DMARC compliant

Data Management

• All data in-transit and at-rest is encrypted.
• Data is typically classified as Category 1

System Availability

• System outage notifications can be sent to client-specified notification list.
• Client service support is available through email, telephone and a self-service portal.
• Maintenance windows are Monday and Friday mornings.

Software Upgrades

• Major releases occur throughout the year, typically once per quarter.
• Minor releases occur typically every other week.
• All clients receive all upgrades according to their license package.

Standard MSA commitments to confidential information include:

Protection of Confidential Information: To the extent permitted by Michigan law, the Receiving Party agrees that during the Term and at any time thereafter, it (a) will use the same level of care to protect the confidentiality of the Disclosing Party's Confidential Information as it does to protect its own Confidential Information, but in no event less than a reasonable degree of care, (b) will not use any Confidential Information of the Disclosing Party except for the purpose of fulfilling its obligations under this Agreement, (c) will not, and will not permit others to, duplicate, transfer, sell, lease, or otherwise make any Confidential Information of the Disclosing Party available to others without the prior written consent of the Disclosing Party, and (d) will not remove, or permit to be removed, any notice indicating the confidential nature of, or the proprietary rights of the Disclosing Party in, the Disclosing Party's Confidential Information. To the extent permitted by Michigan law, the Receiving Party will return all Confidential Information at the earlier of the termination of this Agreement or upon the request of the Disclosing Party.

Components of the System

InfoReady's system includes infrastructure, software, people, procedures and data.

Infrastructure

The collection of physical and virtual resources that supports an overall IT environment, including the physical environment and related structures and hardware that InfoReady uses to provide its Process Automation Platform. The Process Automation Platform is deployed on Infrastructure-as-a-Service provided by Rackspace and AWS. The Infrastructure-as-a-Service environment provides a secure, highly available and scalable infrastructure.

Hardware and software components comprising the Process Automation Platform infrastructure include:

Component	Domestic (U.S.) Customers (AWS)	Domestic (U.S.) Customers (Rackspace)	International Customers (AWS)
Application supported	Review (since May 2023)	Review (until May 2023) Scale	Review
Server hardware	All servers are hosted within AWS in a secure segmented network	All servers are dedicated and hosted within Rackspace in a secure segmented network	All servers are hosted within AWS in a secure segmented network
Network components	Virtual Private Cloud (VPCs)	Virtual Private Cloud (VPCs)	Virtual Private Cloud (VPCs)
Operating systems	Red Hat Enterprise Linux	CentOS	Red Hat Enterprise Linux
Databases	MySQL	MySQL and MariaDB	MySQL
Monitoring systems	AWS Systems Manager	Alert Logic through Rackspace	AWS Systems Manager
Network infrastructure	The network infrastructure is hosted and managed by AWS which includes the following: • Circuits • Switches • Load balancers • Firewalls • Routers • Hardware appliances • Storage arrays	The network infrastructure is hosted and managed by Rackspace which includes the following: • Circuits • Switches • Load balancers • Firewalls • Routers • Hardware appliances • Storage arrays	The network infrastructure is hosted and managed by AWS which includes the following: • Circuits • Switches • Load balancers • Firewalls • Routers • Hardware appliances • Storage arrays

Component	Domestic (U.S.) Customers (AWS)	Domestic (U.S.) Customers (Rackspace)	International Customers (AWS)
Built-in redundancy	Multi-zone hosting within the East and West regions	Rackspace managed backup and multiple location redundancy	Multi-zone hosting within the Southeast Asia and Canada regions
Storage	Amazon S3	Rackspace Storage Area Network	Amazon S3
Security functionality	Firewalls, Virtual Private Network ("VPN"), Intrusion Detection System ("IDS"), Anti-virus detection systems, Internal/External vulnerability scanning and management tools		

Software

InfoReady employs additional programs and operating software used in the development and management of the Process Automation Platform. The significant programs and software include:

Software	Description
System/network monitoring	All computing systems, including server, networking, security, application and database platforms are monitored through InfoReady's monitoring ecosystem.
Support ticketing and workflow management	InfoReady's technical support ticketing and workflow management system manages customer requests, troubleshooting, password resets and related account activities.
Software development	InfoReady uses an issue and project tracking system to track and manage its software development activities.
Vulnerability management	InfoReady uses a third party to perform both automated and manual vulnerability scans.
Access Management	Microsoft Active Directory is used for identity and access management requests.
Redundancy tools	InfoReady leverages service architecture from Rackspace and AWS to ensure data resiliency.
Anti-virus	InfoReady leverages endpoint protection to secure its server and desktop infrastructure. The solution includes malware protection, quarantining and scanning.

Software	Description
Logging	Rackspace and AWS are used to monitor logs from all production systems, to perform analysis on the activity of the environment and to alert InfoReady of possible security incidents.
HR management	InfoReady uses its Process Automation Platform to support its HR function. This includes checklists for performance management, onboarding, offboarding and employee management.

People

InfoReady's organizational structure provides a framework for planning, executing and controlling business operations. Executive and senior leadership play important roles in establishing core values. The organizational structure assigns roles and responsibilities to provide for adequate staffing, security, efficiency of operations and segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel.

InfoReady follows a structured onboarding process to familiarize new employees with InfoReady's tools, processes, systems, security practices, policies and procedures. Employees are provided with the employee handbook and additionally complete at least annual security training.

Processes and Procedures

InfoReady maintains policies and procedures to guide business operations. The procedures include control activities designed to help ensure operations are carried out properly, consistently and efficiently. InfoReady uses a risk management approach to select and develop these control activities. After relevant risks are identified and evaluated, controls are established, implemented, monitored, reviewed and improved when necessary to meet the overall objectives of the organization. Processes and procedures are documented throughout Sections III and IV of this report.

Data

InfoReady serves as a data processor service provider. InfoReady considers its business clients to be data controllers. InfoReady provides controls at each level of data storage, access and transfer. InfoReady has established incident response processes to report and handle events related to security. InfoReady established agreements, including non-disclosure agreements, for preserving the security of information exchanged with external parties.

Data used in the Process Automation Platform is stored and encrypted within databases that are part of the infrastructure as a service environment through Rackspace and AWS. Access to the databases is governed by the applicable application-level access and permission controls within the environments. Data is transferred over SSL/TLS connections.

Data is classified in the following groups:

Classification	Data Classification Description	
Restricted	Definition	Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need. Restricted information includes PII (Personally Identifiable Information), NPI (non-public information) under the protection of laws and/or regulations (HIPAA, GDPR, etc.).
	Potential Impact of Loss	Significant damage would occur if Restricted information were to become available to unauthorized parties either internal or external to InfoReady. Impact could include negatively affecting InfoReady's competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk. Examples include social security numbers, personal financial data, health information, biometric data, etc.
Confidential	Definition	Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by InfoReady.
	Potential Impact of Loss	Significant damage would occur if Confidential information were to become available to unauthorized parties either internal or external to InfoReady. Impact could include negatively affecting InfoReady's competitive position, damaging the company's reputation, violating contractual requirements, and exposing geographic locations of individuals.
Internal Use	Definition	Internal Use information is information originating within or owned by InfoReady or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.

Classification	Data Classification Description	
	Potential Impact of Loss	Moderate damage would occur if Internal Use information were to become available to unauthorized parties either internal or external to InfoReady. Impact could include damaging the company's reputation and violating contractual requirements.
Public	Definition	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.
	Potential Impact of Loss	No damage would occur if Public information were to become available to parties either internal or external to InfoReady. Impact would not be damaging or a risk to business operations.

Data handling based on data classification:

Handling Controls	Restricted Data	Confidential Data	Internal Use Data	Public Data
Non-Disclosure Agreement (NDA)	NDA is required prior to access by non-InfoReady employees.	NDA is recommended prior to access by non-InfoReady employees.	No NDA requirements.	No NDA requirements.
Internal Network Transmission (wired and wireless)	Encryption is required. sFTP is acceptable.	Encryption is recommended. sFTP is acceptable.	No special requirements.	No special requirements.
External Network Transmission (wired and wireless)	Encryption is required. sFTP is acceptable. Remote access should be used only when necessary and only with VPN and two-factor authorization when possible	Encryption is required. sFTP is acceptable.	Encryption is recommended. sFTP is acceptable.	No special requirements.

Handling Controls	Restricted Data	Confidential Data	Internal Use Data	Public Data
Data at Rest (file servers, databases, archives, etc.)	Encryption is required. Logical access controls are required to limit unauthorized use. Physical access restricted to specific individuals.	Encryption is recommended. Logical access controls are required to limit unauthorized use. Physical access restricted to specific groups.	Encryption is recommended. Logical access controls are required to limit unauthorized use. Physical access restricted to specific groups.	Logical access controls are required to limit unauthorized use. Physical access restricted to specific groups.
Mobile devices (iPhone, iPad, USB Drive, etc.)	Encryption is required. Remote wipe must be enabled, if possible.	Encryption is required. Remote wipe must be enabled, if possible.	Encryption is recommended. Remote wipe should be enabled, if possible.	No special requirements.
Email (with and without attachments)	Encryption is required. Do not forward.	Encryption is recommended. Do not forward.	Encryption is recommended. Do not forward.	No special requirements.
Physical Mail	Mark “open” by addressee only. Use certified mail and sealed, tamper-resistant envelopes for external mailings. Delivery confirmation is required. Hand deliver internally.	Mark “open” by addressee only. Use certified mail and sealed, tamper-resistant envelopes for external mailings. Delivery confirmation is required. Hand deliver internally is recommended.	Mail with company interoffice mail, US Mail or other public delivery systems. Use of sealed and tamper-resistant envelopes for external meetings.	No special requirements.
Printers	Verify destination printer and attend printer while printing.	Verify destination printer and attend printer while printing.	Verify destination printer and retrieve printed material without delay.	No special requirements.

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

The security trust services criteria were used to evaluate the suitability of design of controls stated in the description. Security criteria and controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security criteria are included in Section IV of this report. Although the applicable trust services criteria are included in Section IV, they are an integral part of InfoReady's Process Automation Platform.

Control Environment

The control environment reflects the overall attitude and awareness of management and personnel concerning the importance of controls and the emphasis given to controls in InfoReady's policies, procedures and actions. The control environment serves as the foundation for the other components of internal controls. The organizational structure, separation of job responsibilities by departments and business function and documentation of policies and procedures, are the methods used to define and implement operational controls.

InfoReady's executive team has the ultimate responsibility for overseeing the affairs of InfoReady. The executive team is responsible for directing and controlling operations and for establishing, communicating and monitoring control policies and procedures. The executive team focuses on maintaining internal controls and the integrity and ethical values of personnel. Organizational values and behavioral standards are communicated to personnel through policy statements and guidelines during new-hire orientation and are also available for review on an ongoing basis. InfoReady maintains an open-access policy within the company to facilitate open and frequent communication.

Policies and Procedures

InfoReady's policies and procedures are designed to achieve compliance with the AICPA's Trust Services Criteria for Security. InfoReady maintains the following security and related policies and procedures:

- Breach Notification
- Building Security
- Change Management
- Contingency Plan
- Disposal of External Media / Hardware
- Domestic Hosting Oversight and Management
- Employee Responsibilities - Information Technology
- Encryption
- Identification and Authentication
- Information System Activity Review
- Malicious Code
- Network Connectivity
- Retention / Destruction of Medical Information

- Securing Management Process
- Security Awareness and Training
- Specific Protocols and Devices
- Telecommuting

Control Activities

Control activities have been developed at inception and as the business evolves. When risks are identified, management acts to investigate the risk and develops controls with the objective to reduce the identified risk. After the controls are implemented, management reviews the effectiveness to ensure the control is meeting the objective.

Risk Assessment Process

InfoReady regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security based on the applicable trust services criteria set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

InfoReady has a documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, compliance and procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. The risk assessment procedures address the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification or destruction of the system and the information it processes, stores and transmits. The risk assessment procedures are performed annually or as significant changes to the information system or environment of operation (including identification of new threats or vulnerabilities) are identified.

Information and Communication Systems

Information regarding the design and operation of the system, system boundaries, and responsibilities related to security are communicated internally and externally on a consistent basis, especially as changes occur.

Information Security

InfoReady has established formal written policies and practices for all significant functions and processes to help ensure that assets are safeguarded, and system resources and data are protected from unauthorized physical and logical access with respect to security. The policies and procedures are reviewed and approved by the Security Officer on an annual basis. The policies and procedures are made available to employees during new hire orientation and through the company shared drive.

Logical access is controlled and monitored using defined hardening guidelines, user authorization processes, password-based authentication, and job-defined access restrictions.

Physical Security and Environmental Safeguards

InfoReady relies on Rackspace and AWS to provide physical security and environmental safeguard controls around the data centers that host the Process Automation Platform. InfoReady does not have a central office and all employees work remotely.

Personnel Security

Prior to employment, personnel are verified against regulatory screening databases, including credit, criminal and employment checks as permitted by applicable law. New employees are required to review and acknowledge their personal obligations to data security as documented in InfoReady's policies and procedures. All employees are required to review and sign a confidentiality and non-competition agreement. Job descriptions are used to support positions within InfoReady. Once employed, employees are subject to InfoReady's procedures for accessing systems and sanctions for violating InfoReady's policies and procedures.

InfoReady leases employees from GDI Infotech. These employees are subject to GDI Infotech's hiring policies and procedures. InfoReady is responsible for granting access to the leased employees, monitoring their performance and ensuring they follow the policies and procedures established by InfoReady.

Business Systems Access Management

Access to InfoReady's Business Systems is granted to new employees upon hiring via InfoReady's employee management workflow within the Scale platform. Employees are granted a username and password and do not share accounts. Upon leaving InfoReady, access to all InfoReady Business Systems is revoked via InfoReady's employee management platform.

Production System Access Management

Access to the production system is limited to authorized individuals. Access is reviewed annually, at a minimum, to ensure access is restricted to authorized individuals. A provisioning process is in place for establishing, activating, modifying, reviewing, disabling and removing user accounts. The level of access is based on the minimum necessary amount of access for the user to meet their job requirements. Contractors and third parties who are granted access to the production system follow defined access procedures which includes approval, monitor of usage, logging of activity and removal of access when the job or project is complete.

Process Automation Platform Client Access

Access to the Process Automation Platform occurs over HTTPS (encrypted HTTP traffic). To access the application the user must navigate to the website and sign in with a username and password unique to that user. The Process Automation Platform is capable of being configured to support single sign on through other access management tools. When using single sign-on to access the Process Automation Platform the logs of user access reside with the customer. InfoReady logs user access for all other users authenticating with the Process Automation Platform.

InfoReady has implemented role-based security within the Process Automation Platform to limit and control access within the system. Initial client access is approved by InfoReady. Clients are then responsible for adding, reviewing and removing users.

Password controls, such as minimum length and a combination of letters, numbers and special characters are documented and configured. Additional controls include account lock out after a given number of access attempts and account inactivity timeouts.

Encryption

InfoReady relies on HTTPS with SSL/TLS encryption for all application sessions within the Process Automation Platform. All sessions are secured using 256 bit AES encryption using 2048 bit keys.

Full disk encryption is enforced for laptops.

Antivirus

Where technically applicable, InfoReady uses a real-time antivirus solution to protect its devices against viruses, worms, trojan horses and other forms of malicious code that may cause damage.

Access Logs

InfoReady logs system access and activity within the production environment and the Process Automation Platform. Activities and events are reviewed on an ad-hoc basis.

Change Management

Change management is the process for managing the implementation of various types of changes to validated systems. This includes hardware, software, application and system patching, services or related documentation. InfoReady has a documented change management process to help ensure the delivery of consistent and reliable services.

The change management process begins with a request being submitted to the Change Management Committee. Upon approval from the Change Management Committee, a test plan is developed to test the changes in a pre-production test environment. Upon final approval from the Change Management Committee, changes are put into production.

Problem Management

A problem management process is in place to help ensure that client service issues related to security are identified, reported, reviewed and resolved in a timely manner. A problem can be identified internally or by a client. Issues are tracked and monitored until resolved.

Vulnerability Management

As part of the risk management process, the following are completed:

- Penetration testing – annually by a third party
- Vulnerability scans – quarterly
- Web app scans – as significant changes are made

InfoReady has a defined remediation process to ensure any necessary remediation is completed timely.

Backups

Incremental backups of all servers containing client data are completed daily. Weekly a full backup of all servers containing client data is completed. Backup data is maintained for six months. Testing of backup data is completed on an as needed basis, but at a minimum annually as part of the contingency plan.

Business Continuity

To ensure continuity of service, InfoReady maintains a disaster recovery and business continuity plan. The plan is available and maintained to protect critical business processes from the effects of major failures or disasters. The plan is tested annually.

Monitoring Controls

InfoReady has established monitoring controls to consider whether the controls are operating as intended, and whether they are modified timely as appropriate for changes in conditions or risks facing the company. Regular meetings and a company-wide risk assessment are used to monitor and assess the efficiency and effectiveness of key processes and controls and identify potential performance issues.

InfoReady has defined and implemented relevant procedures to control the activities of vendors and other contract personnel to protect the company's assets. InfoReady enters into Business Associate Agreements with vendors that specifies the applicable requirements for information use and sharing. Third-party vendor systems are subject to review as part of the vendor risk management process. This includes reviews of security measures implemented by third parties and reviews of contracts, Business Associate Agreements and Service Level Agreements as applicable.

Complementary Subservice Organization Controls

InfoReady uses subservice organizations for the following services:

Subservice Organization	Services Provided
Amazon Web Services (AWS)	Hosting and Infrastructure-as-a-Service
Freshdesk	External ticketing system
GDI Infotech, Inc.	Professional Employer Organization providing office space and HR coordination and support
Microsoft	Email, calendar, and administration
Rackspace	Hosting and Infrastructure-as-a-Service
Veracode	Application security testing

InfoReady's controls related to the Process Automation Platform covers only a portion of the overall internal control for each user entity of InfoReady. Each user entity's internal control over security must be evaluated in conjunction with InfoReady's controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

#	Complementary Subservice Organization Control	Related Criteria
1	Subservice organizations are responsible for notifying InfoReady of any security incidents related to their system.	CC2.3, CC7.3, CC7.4
2	GDI Infotech, Inc. is responsible for ensuring that policies and procedures are in place to attract and develop individuals with the necessary background and experience to meet their job requirements.	CC1.4
3	Subservice organizations are responsible for ensuring that logical access to their system is restricted to authorized personnel and for implementing controls to ensure the prevention and detection of unauthorized access.	CC6.1, CC6.2, CC6.3, CC6.6

#	Complementary Subservice Organization Control	Related Criteria
4	Subservice organizations are responsible for ensuring logical and physical security controls are in place to restrict access to production systems, backup data and media.	CC6.4
5	Subservice organizations are responsible for ensuring that antivirus or antimalware solutions are installed to detect or prevent unauthorized or malicious software.	CC6.8
6	Subservice organizations are responsible for having controls in place to ensure that changes to system components, patches, and other updates are appropriately authorized, tested, implemented and documented.	CC8.1

Complementary User Entity Controls

In designing its system, InfoReady has contemplated that certain complementary controls would be implemented by user organizations to meet certain criteria applicable to security. The list of complementary user entity controls listed below is not and should not be considered a comprehensive list of internal controls that should be employed by the client of InfoReady. Other internal controls may be required at user organizations.

#	Complementary User Entity Control	Related Criteria
1	User entities are responsible for monitoring user accounts to ensure access is assigned to authorized individuals and that access is removed in a timely manner for terminated individuals	CC6.2
2	User entities are responsible for establishing controls to ensure appropriate design and implementation of security architecture for devices maintained by the entity.	CC6.6
3	User entities are responsible for establishing controls to ensure data is protected and secured during transmission, movement or removal.	CC6.7

Responsibilities of user entities not tied directly to SOC 2 criteria.

User Entity Responsibility
User entities are responsible for establishing controls to have appropriate personnel available to report service/operation-related issues and to discuss them with InfoReady.

User Entity Responsibility
User entities are responsible for monitoring their open sessions and enforcing a logout at their desktops after a certain period of inactivity within the Process Automation Platform.

The list of user entity control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user entities. Other controls may be required at user entities. Therefore, each client's system of internal controls must be evaluated in conjunction with the internal control structure described in the report.

Changes Since the Previous Report

In May 2023, InfoReady migrated its hosting and infrastructure for the Review application to AWS. The Scale application is being sunset and continues to be hosted at Rackspace. See the infrastructure section for applicable changes to the infrastructure in the transition from Rackspace to AWS. The control procedures were impacted by the change.

Original Control	Current Controls
(24) Rackspace manages the backups for InfoReady. Incremental backups of all servers containing client data are completed daily. Weekly a full backup of all servers containing client data is completed. Backup data is maintained for one year.	(24) The hosting providers manage the backups for InfoReady. Incremental backups of all servers containing client data are completed daily. Weekly a full backup of all servers containing client data is completed. Backup data is maintained for one year.
(40) Databases, backups and logs are encrypted at rest using industry standard encryption algorithms provided by Rackspace as part of the hosting services.	(40) Databases, backups and logs are encrypted at rest using industry standard encryption algorithms provided by Rackspace and AWS as part of the hosting services.

Identified System Incidents

As of October 31, 2023, there were no significant system incidents impacting the service commitments and system requirements of the Process Automation Platform during the prior year.

In Closing

We have not omitted or distorted information relevant to InfoReady while acknowledging that this description has been prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

Section IV – Trust Services Criteria Relevant to Security, Trust Services Criteria for Security Mapped to ISO 27001 Requirements, Related Controls and Tests of Controls

Applicable Trust Services Criteria Relevant to Security

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

Criteria	Description
Security	Security refers to the protection of: • Information during its collection or creation, use, processing, transmission, and storage and • Systems that use electronic information to process, transmit or transfer, and store information to enable the achievement of the company's service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

The ISO 27001 requirements mapped to the Trust Services Criteria for Security was completed using mappings provided by the American Institute of Certified Public Accountants. The mapping includes only the ISO 27001 requirements that are mapped to the Trust Services Criteria for Security and not a complete listing of the ISO 27001 requirements.

Criteria and Related Controls for Systems and Applications

On the pages that follow, the applicable trust services criteria and the controls to meet the trust services criteria and the applicable trust services criteria mapped to the corresponding ISO 27001 requirements have been specified by and are the responsibility of InfoReady. The sections "Service Auditor's Tests of Controls" and "Test Results" are the responsibility of the Service Auditor.

For tests of controls requiring the use of Information Produced by the Entity (IPE) (e.g., 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 IPE to address the completeness, accuracy and data integrity of the date or reports used:

1. Inspected the source of the IPE,
2. Inspected the query, script or parameters used to generate the IPE,
3. Tied data between the IPE and the source, and/or
4. Inspected the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate and maintained its integrity

Furthermore, in addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., reviews of user access listings); we inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy and integrity of the data or reports.

Testing Performed and Results of Tests of Entity Level Controls

In planning the nature, timing and extent of our testing of the controls specified by InfoReady, we considered the aspects of InfoReady's control environment, risk assessment process, communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

Sample sizes were selected using professional judgement and based on the nature (e.g., automated or manual) of the controls, the frequency of the control and the available population.

Tests performed on the control design and operating effectiveness detailed in this section are described below:

Test	Description
Observation	Observed application of specific control structure activities, including observation of the existence and availability of specific, written control structure policies and procedures, or observed application of specific control structure activities within InfoReady's operations to ascertain whether control policies and procedures were adhered to.
Corroborative Inquiry	Conducted inquiries of management and corroborated responses with appropriate personnel. Also, conducted inquiries of personnel responsible for carrying out the specific control policies and procedures in the specific InfoReady operations unit and area, and corroborated responses with other personnel responsible for carrying out these procedures.
Evidential Material	Inspected documents and reports indicating performance of the control structure, policy, or procedure, and a selection of system input, output and edit reports to ascertain whether controls over systems were operating as described and the control policies and procedures were operating effectively. Also, to ascertain whether the transactions and associated reports and deliverables were prepared, approved and maintained in accordance with the specific control policies and procedures and to evaluate whether the control policies and procedures were operating effectively.
Walkthrough	Re-performed application of the control structure, policy, or procedure or performed a walkthrough of the specific control activity on current data to ascertain that the control policies and procedures were implemented and operating effectively.

Results of Testing Performed

We reviewed the controls listed below in order to determine whether InfoReady had designed and implemented a system of controls to adequately address the control criteria. The results of the testing of the control environment and control policies and procedures were sufficient to conclude that the controls were operating effectively to provide reasonable, but not absolute, assurance that the control objectives were achieved during the reporting period. The results of our audit are discussed below.

Control Number	Control Activity Specified by InfoReady	Service Auditor's Tests of Controls*	Results of Testing*	Trust Services Criteria	ISO 27001 Requirement
1	InfoReady has documented the code of business conduct and ethical standards.	Obtained and inspected employee handbook on business conduct and ethical standards covering topics such as in-office conduct and non-discrimination standard.	No exceptions noted.	CC1.1	5.1
2	InfoReady's code of business conduct includes a sanctions policy for personnel who violate the code of business conduct. The sanctions policy is applied to personnel who violate the code of business conduct.	Obtained and inspected employee handbook noting language covering violations of the code of conduct.	No exceptions noted.	CC1.1; CC1.5	5.1
3	Where permitted by applicable law, prior to employment, personnel (excluding interns) undergo background screening including verification against regulatory screening databases.	Obtained and inspected employee background checks completed for all new hires during the period.	No exceptions noted.	CC1.1; CC1.4	5.1 7.1 7.2
4	On their first day of employment at InfoReady, all employees are required to review and acknowledge their receipt of the policies and procedures. All new employees are required to review and sign an intellectual property, confidentiality, non-competition and non-solicitation agreement.	Obtained and inspected signed acknowledgements for all new hires during the period.	No exceptions noted.	CC1.1; CC1.3; CC1.5; CC2.2	4.3 5.1 5.3

Control Number	Control Activity Specified by InfoReady	Service Auditor's Tests of Controls*	Results of Testing*	Trust Services Criteria	ISO 27001 Requirement
5	InfoReady executive staff 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 revises these when necessary to support the achievement of objectives.	Obtained and inspected organizational chart maintained by the organization.	No exceptions noted.	CC1.3	4.3 5.1 5.3
6	There are written job descriptions to inform personnel of their duties that are distributed to each employee with respect to their position. Reporting relationship and organizational structures are reviewed periodically by the executive staff as part of company planning and adjusted as needed based on changing commitments and requirements.	Obtained and inspected job descriptions and the organizational chart maintained by the organization.	No exceptions noted.	CC1.3; CC1.4; CC5.3	4.3 5.1 5.2 5.3 7.1 7.2 10.1a
7	InfoReady has established formal written policies and practices for all significant functions and processes to help ensure that assets are safeguarded, and system resources and data are protected from unauthorized physical and logical access with respect to security. The policies include physical and logical security requirements, provisioning and authentication of users, data classification, risk assessment, incident response, change management and the contingency plan.	Obtained and inspected policies and procedures noting relevant sections.	No exceptions noted.	CC1.3; CC2.1; CC2.2; CC5.1; CC5.2; CC5.3; CC6.1; CC6.4; CC6.5; CC9.1	4.3 5.1 5.2 5.3 6.1.3b 6.2 7.2 7.3 7.4 8.3 10.1a

Control Number	Control Activity Specified by InfoReady	Service Auditor's Tests of Controls*	Results of Testing*	Trust Services Criteria	ISO 27001 Requirement
8	The relevant security policies and procedures are reviewed and approved by the COO on an annual basis. A complete list is detailed in Section III.	Obtained and inspected Information Security Policy noting annual review by the COO.	No exceptions noted.	CC1.3; CC2.1; CC5.1; CC5.2; CC5.3	4.3 5.1 5.2 5.3 6.1.3b 6.2 7.2 8.3 10.1a
9	Hiring decisions are based on various factors, including educational background, prior relevant experience, past accomplishments and evidence of integrity and ethical behavior.	Obtained and inspected evidence of qualifications for all new hires during the period.	No exceptions noted.	CC1.4	7.1 7.2
10	Management provides continued training about its commitments and requirements for personnel to support the achievement of objectives.	Obtained and inspected evidence of security training completed by all new hires during the period.	No exceptions noted.	CC1.4; CC2.2	7.1 7.2 7.3 7.4
11	The employee performance monitoring process includes annual reviews to provide developmental feedback.	Obtained and inspected documents used in the performance review process for a sample of employees.	No exceptions noted.	CC1.4	7.1 7.2

Control Number	Control Activity Specified by InfoReady	Service Auditor's Tests of Controls*	Results of Testing*	Trust Services Criteria	ISO 27001 Requirement
12	InfoReady's COO and the Confidentiality/Security Team are charged with establishing, maintaining and enforcing the overall policies and procedures.	Obtained and inspected policies and procedures noting COO and Confidentiality/Security Team are responsible for establishing, maintaining and enforcing the overall policies and procedures.	No exceptions noted.	CC1.5; CC2.2; CC5.1; CC5.2; CC5.3; CC9.2	5.2 6.1.3b 6.2 7.2 7.3 7.4 8.3 10.1a
13	InfoReady has a documented risk assessment policy that addresses purpose, scope, responsibilities, and procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. The risk assessment procedures address the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification or destruction of the system and the information it processes, stores or transmits. The risk assessment procedures are performed annually or as significant changes to the information system or environment of operation (including identification of new threats or vulnerabilities) are identified.	Obtained and inspected risk assessment policy. Obtained and inspected annual risk assessment completed.	No exceptions noted.	CC2.1; CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC7.1; CC7.3; CC7.4; CC9.1; CC9.2	5.1c 6.1.1 6.1.2 6.2c 7.1 7.2 7.4 8.2 8.3 9.1 9.2 9.3 10.1 10.2

Control Number	Control Activity Specified by InfoReady	Service Auditor's Tests of Controls*	Results of Testing*	Trust Services Criteria	ISO 27001 Requirement
14	Network and application vulnerability scans are performed by InfoReady to help ensure the overall security of the production environment as well as consistency with InfoReady policies. Identified vulnerabilities are remediated.	Obtained and inspected vulnerability scans completed during the period to ensure the overall security of the production environment.	No exceptions noted.	CC2.1; CC3.1; CC3.2; CC3.4; CC4.1; CC4.2; CC5.2; CC7.1; CC7.2; CC7.4	5.1c 6.1.1 6.1.2 6.1.3b 6.2c 7.1 7.2 7.4 8.2 8.3 9.1 9.2 9.3 10.1 10.2
15	Internal and external users have been provided with information on how to report security failures, incidents, concerns and other complaints to appropriate personnel.	Inspected communication channels for internal and external users to report security failures, incidents, concerns or other complaints to appropriate personnel.	No exceptions noted.	CC2.2; CC2.3; CC7.2	7.3 7.4
16	Breach notification policies and procedures are in place that includes escalation plans based on the nature and severity of the breach.	Obtained and Inspected breach notification policies and procedures.	No exceptions noted.	CC2.2; CC2.3; CC4.2; CC6.8; CC7.3; CC7.4; CC7.5	7.1 7.3 7.4 9.1 9.2 10.1 10.2

Control Number	Control Activity Specified by InfoReady	Service Auditor's Tests of Controls*	Results of Testing*	Trust Services Criteria	ISO 27001 Requirement
17	InfoReady's security commitments are communicated to external users, as appropriate.	Obtained and inspected InfoReady's subscription agreement and recognized language for security commitments.	No exceptions noted.	CC2.3	7.4
18	Agreements are established with service providers and business partners that include clearly defined terms, conditions, and responsibilities for service providers and business partners.	Obtained and inspected agreements with service providers.	No exceptions noted.	CC2.3; CC9.2	7.4
19	A problem management process is in place to help ensure that customer service issues related to security are identified, reported, reviewed and resolved in a timely manner.	Obtained and inspected communication channels for customers to report service issues related to security. Obtained and inspected ticketing system used to review and resolve issues.	No exceptions noted.	CC3.1; CC3.2; CC3.4; CC4.2; CC7.5	5.1c 6.1.1 6.1.2 6.2c 7.1 7.4 8.2 8.3 9.1 9.2 10.1b 10.1d 10.1e

Control Number	Control Activity Specified by InfoReady	Service Auditor's Tests of Controls*	Results of Testing*	Trust Services Criteria	ISO 27001 Requirement
20	A variety of security utilities are used to identify and detect possible security threats and incidents. E-mails are sent to designated staff when a component or service has failed one of the configured thresholds.	Obtained and inspected notification received from security utilities in place to monitor the network.	No exceptions noted.	CC3.2; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC6.6; CC6.8; CC7.1; CC7.2; CC7.4	5.1c 6.1.1 6.1.2 6.1.3b 6.2 7.1 7.2 7.4 8.2 8.3 9.1 9.2 9.3 10.1 10.2
21	Third-party vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated.	Obtained and inspected SOC 2 reports obtained and reviewed.	No exceptions noted.	CC3.2; CC9.2	5.1c 6.1.1 6.1.2 8.2 8.3
22	Users, groups and computers have defined access requirements based on business need.	Inspected access management noting defined access requirements.	No exceptions noted.	CC3.3; CC5.1; CC6.1; CC6.3	6.1.2 6.1.3b 6.2 8.3

Control Number	Control Activity Specified by InfoReady	Service Auditor's Tests of Controls*	Results of Testing*	Trust Services Criteria	ISO 27001 Requirement
23	All access attempts and validated sessions for the Process Automation Platform are logged.	Inspected log from the Process Automation Platform noting user access is logged.	No exceptions noted.	CC4.1	7.2 9.1 9.2 9.3 10.2
24	The hosting providers manage the backups for InfoReady. Incremental backups of all servers containing client data are completed daily. Weekly a full backup of all servers containing client data is completed. Backup data is maintained for one year.	Obtained and inspected evidence of backup configuration and logs of the backup status.	No exceptions noted.	CC4.2; CC7.4; CC7.5	7.1 7.4 9.1 9.2 10.1 10.2
25	The contingency plan, which includes business continuity, disaster recovery and restoration of backups is tested annually.	Obtained and inspected contingency plan and evidence of annual testing of the plan.	No exceptions noted.	CC4.2; CC7.5	7.4 9.1 9.2 10.1b 10.1d 10.1e
26	InfoReady has implemented role-based security to limit and control access within the Process Automation Platform.	Obtained and inspected user access roles within the Process Automation Platform.	No exceptions noted.	CC6.1; CC6.2; CC6.3	
27	Employees are granted logical and physical access to in-scope systems based on documented approvals by appropriate management personnel.	Obtained and inspected user access requests for all new hires during the period.	No exceptions noted.	CC6.1; CC6.2; CC6.3	

Control Number	Control Activity Specified by InfoReady	Service Auditor's Tests of Controls*	Results of Testing*	Trust Services Criteria	ISO 27001 Requirement
28	Password controls such as change frequency, complexity and password reuse/history are documented and configured to enforce access control for the corporate domain.	Obtained and inspected password requirements.	No exceptions noted.	CC6.1	
29	Password controls such as change frequency, complexity and password reuse/history are documented and configured to enforce access control for accessing the Process Automation Platform.	Obtained and inspected password requirements.	No exceptions noted.	CC6.1	
30	User access is reviewed annually to verify whether individuals access is necessary for their job functions and to identify the existence of inappropriate accounts.	Obtained and inspected user access review completed during the period.	No exceptions noted.	CC6.1; CC6.2; CC6.3	
31	Access to the system is disabled for terminated employees in a timely manner.	Inspected termination checklist noting access has been disabled in a timely manner for all terminated employees during the period.	No exceptions noted.	CC6.1; CC6.2; CC6.3	
32	Full disk encryption is used to protect the confidentiality of information on laptops. Remote access to the production environment is done through an encrypted VPN connection.	Obtained and inspected settings in place for full disk encryption and use of encrypted VPN connection.	No exceptions noted.	CC6.1; CC6.6; CC6.7	

Control Number	Control Activity Specified by InfoReady	Service Auditor's Tests of Controls*	Results of Testing*	Trust Services Criteria	ISO 27001 Requirement
33	InfoReady maintains a board of directors. The board of directors holds meetings quarterly to discuss the business and provide guidance regarding the direction of the business and its activities.	Inspected listing of board of directors and meeting minutes for all board meetings taking place during the period.	No exceptions noted.	CC1.2	5.1c 5.1h
34	All sessions of the Process Automation Platform are encrypted using 256 bit AES encryption using 2048 bit keys.	Inspected access to the platform noting 256 bit AES encryption using 2048 bit keys.	No exceptions noted.	CC6.1; CC6.6; CC6.7	
35	To access the Process Automation Platform the user must navigate to the website and sign in with a user name and password unique to that user.	Inspected Process Automation Platform noting use of user name and password to access the platform.	No exceptions noted.	CC6.1	
36	Separate environments are used for development and production.	Obtained and inspected evidence of development and production environments in place.	No exceptions noted.	CC8.1	7.5.3e
37	InfoReady relies on Rackspace and AWS to provide physical security and environmental safeguard controls around the data centers that host the Process Automation Platform. InfoReady obtains and reviews SOC 2 reports for Rackspace and AWS to ensure appropriate controls are in place.	Inspected evidence of management's oversight of Rackspace and AWS.	No exceptions noted.	CC6.4	

Control Number	Control Activity Specified by InfoReady	Service Auditor's Tests of Controls*	Results of Testing*	Trust Services Criteria	ISO 27001 Requirement
38	Formal data retention and disposal procedures are in place to guide the secure disposal of the company's and customers' data.	Obtained and inspected policies and procedures for data retention and disposal.	No exceptions noted.	CC6.5	
39	External points of connectivity are protected by a firewall complex defense to prevent unauthorized external users from gaining access to the organization's internal systems and devices.	Obtained and inspected network diagram noting firewall in place.	No exceptions noted.	CC6.6; CC6.7; CC6.8	
40	Databases, backups and logs are encrypted at rest using industry standard encryption algorithms provided by Rackspace and AWS as part of the hosting services.	Obtained and inspected contract with Rackspace and AWS and SOC 2 review forms completed to ensure appropriate encryption controls are in place at Rackspace and AWS.	No exceptions noted.	CC6.6; CC6.7	
41	Process Automation Platform access occurs over HTTPS (encrypted HTTP traffic).	Inspected access to the platform noting use of HTTPS.	No exceptions noted.	CC6.6; CC6.7	
42	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.	Obtained and inspected logs of events and notifications received from tools used in monitoring system infrastructure components	No exceptions noted.	CC6.6; CC6.8; CC7.1; CC7.2; CC7.3	7.4 9.1

Control Number	Control Activity Specified by InfoReady	Service Auditor's Tests of Controls*	Results of Testing*	Trust Services Criteria	ISO 27001 Requirement
43	Where technically applicable, InfoReady uses a real-time antivirus solution to protect against viruses, works, trojan horses and other forms of malicious code that may cause damage. Anti-virus includes auto-update features maintaining current virus definitions.	Obtained and inspected antivirus solution in place at the organization.	No exceptions noted.	CC6.8; CC7.1; CC7.2	9.1
44	The risk management program includes the use of insurance to minimize the financial impact of any loss events.	Obtained and inspected copy of insurance policy.	No exceptions noted.	CC9.2	
45	HTTPS, TLS and related encryption technologies are deployed for transmission of confidential or sensitive information over public networks.	Inspected encryption technologies used for transmission of confidential or sensitive information over public networks.	No exceptions noted.	CC6.7	
46	Formally documented change management procedures are in place to govern the modification and maintenance of production systems.	Obtained and inspected change management policy.	No exceptions noted.	CC8.1	7.5.3e
47	As part of the risk assessment process, InfoReady considers the risk of fraud as it relates to the service objectives of the Company.	Obtained and inspected risk assessment noting fraud being considered in the risk process.	No exceptions noted.	CC3.3	6.1.2

Control Number	Control Activity Specified by InfoReady	Service Auditor's Tests of Controls*	Results of Testing*	Trust Services Criteria	ISO 27001 Requirement
48	A third party is used to perform external and application level penetration testing annually at a minimum.	Obtained and inspected annual penetration test completed.	No exceptions noted.	CC4.1; CC7.1; CC7.3	7.2 7.4 9.1 9.2 9.3 10.2
49	InfoReady requires a change request to be completed for all changes. The change request requires approval from the Change Management Committee.	Obtained and inspected change request and approval for a sample of changes during the period.	No exceptions noted.	CC8.1	7.5.3e
50	Testing is completed as part of the quality assurance process prior to implementing the change.	Obtained and inspected testing completed for a sample of changes during the period.	No exceptions noted.	CC8.1	7.5.3e
51	Prior to implementing the change, the Change Management Committee completes a final review and approval.	Obtained and inspected final review and approval by Change Management Committee for a sample of changes during the period.	No exceptions noted.	CC8.1	7.5.3e
52	As part of the change management process, rollback procedures are defined and reviewed prior to implementing the change.	Obtained and inspected rollback procedures for a sample of changes during the period.	No exceptions noted.	CC8.1	7.5.3e
53	The ability to implement a change is limited to the Operations Engineer and Operations Lead.	Obtained and inspected users with access to implement a change.	No exceptions noted.	CC8.1	7.5.3e

Control Number	Control Activity Specified by InfoReady	Service Auditor's Tests of Controls*	Results of Testing*	Trust Services Criteria	ISO 27001 Requirement
54	Release notes, for major releases only, are available to customers to communicate changes made to the Process Automation Platform.	Obtained and inspected release notes for a sample of changes during the period.	No exceptions noted.	CC8.1	7.5.3e

***Testing includes inquiry of management that the control procedure is in place.**

Trust Services Criteria for Security

Criteria	Criteria Description	Control Activity
CC1.0 Control Environment		
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	1; 2; 3; 4
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	33
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	4; 5; 6; 7; 8
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	3; 6; 9; 10; 11
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	2; 4; 12
CC2.0 Communication and Information		
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	7; 8; 13; 14
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	4; 7; 10; 12; 15; 16
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	15; 16; 17; 18
CC3.0 Risk Assessment		
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	13; 14; 19

Criteria	Criteria Description	Control Activity
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	13; 14; 19; 20; 21
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	13; 22; 47
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	13; 14; 19; 20
CC4.0 Monitoring Activities		
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	13; 14; 20; 23; 48
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	14; 16; 19; 20; 24; 25
CC5.0 Control Activities		
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	7; 8; 12; 20; 22
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	7; 8; 12; 14; 20
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	6; 7; 8; 12
CC6.0 Logical and Physical Access Controls		
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	7; 22; 26; 27; 28; 29; 30; 31; 32; 34; 35

Criteria	Criteria Description	Control Activity
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.	26; 27; 30; 31
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.	22; 26; 27; 30; 31
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	7; 37
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.	7; 38
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	20; 32; 34; 39; 40; 41; 42
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.	32; 34; 39; 40; 41; 45
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	16; 20; 39; 42; 43
CC7.0 System Operations		
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	13; 14; 20; 42; 43; 48

Criteria	Criteria Description	Control Activity
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	14; 15; 20; 42; 43
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.	13; 16; 42; 48
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.	13; 14; 16; 20; 24
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	16; 19; 24; 25
CC8.0 Change Management		
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	36; 46; 49; 50; 51; 52; 53; 54
CC9.0 Risk Mitigation		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	7; 13
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	12; 13; 18; 21; 44