



SOC 2 Type 2 Report

0965688 BC LTD

January 1, 2023 to April 15, 2023

Next Report Issue Date: May 31, 2024

A Type 2 Independent Service Auditor's Report on Controls Relevant to Security



AUDIT AND ATTESTATION BY



AICPA NOTICE:

You may use the SOC for Service Organizations - Service Organizations Logo only for a period of twelve (12) months following the date of the SOC report issued by a licensed CPA. If after twelve months a new report is not issued, you must immediately cease use of the SOC for Service Organizations - Logo.

The next report would be issued on May 31, 2024 subject to observation and examination by Prescient Assurance.

Table of Contents

Management's Assertion	6
Independent Service Auditor's Report	9
Scope	9
Service Organization's Responsibilities	9
Service Auditor's Responsibilities	10
Inherent Limitations	10
Opinion	11
Restricted Use	11
System Description	13
DC 1: Company Overview and Types of Products and Services Provided	14
DC 2: The Principal Service Commitments and System Requirements	15
DC 3: The Components of the System Used to Provide the Services	16
3.1 Primary Infrastructure	16
3.2 Primary Software	16
3.3 People	16
3.4 Security Processes and Procedures	17
3.5 Data	17
3.6 Third Party Access	17
3.7 System Boundaries	17
DC 4: Disclosures About Identified Security Incidents	18
DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved	18
5.1 Integrity and Ethical Values	18
5.2 Commitment to Competence	18
5.3 Management's Philosophy and Operating Style	18
5.4 Organizational Structure and Assignment of Authority and Responsibility	18
5.5 Human Resource Policies and Practices	19
5.6 Security Management	19
5.7 Security and Privacy Policies	19
5.8 Personnel Security	19
5.9 Physical Security and Environmental Controls	20
5.10 Change Management	20
5.11 System Monitoring	20
5.12 Incident Management	20
5.13 Data Backup and Recovery	20
5.14 System Account Management	20
5.15 Risk Management Program	20
5.15.1 Data Classification	20



5.15.2 Risk Management Responsibilities	21
5.15.3 Risk Management Program Activities	21
5.15.4 Integration with Risk Assessment	21
5.16 Information and Communications Systems	21
5.17 Data Communication	21
5.18 Monitoring Controls	21
DC 6: Complementary User Entity Controls (CUECs)	22
DC 7: Complementary Subservice Organization Controls (CSOCs)	23
DC 8: Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant	24
DC 9: Disclosures of Significant Changes in Last 1 Year	24
Testing Matrices	25
Tests of Operating Effectiveness and Results of Tests	26
Scope of Testing	26
Types of Tests Generally Performed	26
General Sampling Methodology	27
Reliability of Information Provided by the Service Organization	28
Test Results	28

SECTION 1

Management's Assertion



PROCOGIA

Management's Assertion

We have prepared the accompanying description of 0965688 BC LTD's system throughout the period January 1, 2023, to April 15, 2023, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report. The description is intended to provide report users with information about 0965688 BC LTD's system that may be useful when assessing the risks arising from interactions with 0965688 BC LTD's system, particularly information about system controls that 0965688 BC LTD has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.


0965688 BC LTD uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at 0965688 BC LTD, to achieve 0965688 BC LTD's service commitments and system requirements based on the applicable trust services criteria. The description presents 0965688 BC LTD's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of 0965688 BC LTD'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 0965688 BC LTD, to achieve 0965688 BC LTD's service commitments and system requirements based on the applicable trust services criteria. The description presents 0965688 BC LTD's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of 0965688 BC LTD's controls.



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

- a. The description presents 0965688 BC LTD's system that was designed and implemented throughout the period January 1, 2023, to April 15, 2023, in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period January 1, 2023 to April 15, 2023, to provide reasonable assurance that 0965688 BC LTD's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of 0965688 BC LTD's controls during that period.
- c. The controls stated in the description operated effectively throughout the period January 1, 2023, to April 15, 2023, to provide reasonable assurance that 0965688 BC LTD's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of 0965688 BC LTD's controls operated effectively throughout the period.

DocuSigned by:

-----85C0B01E879D4CE-----

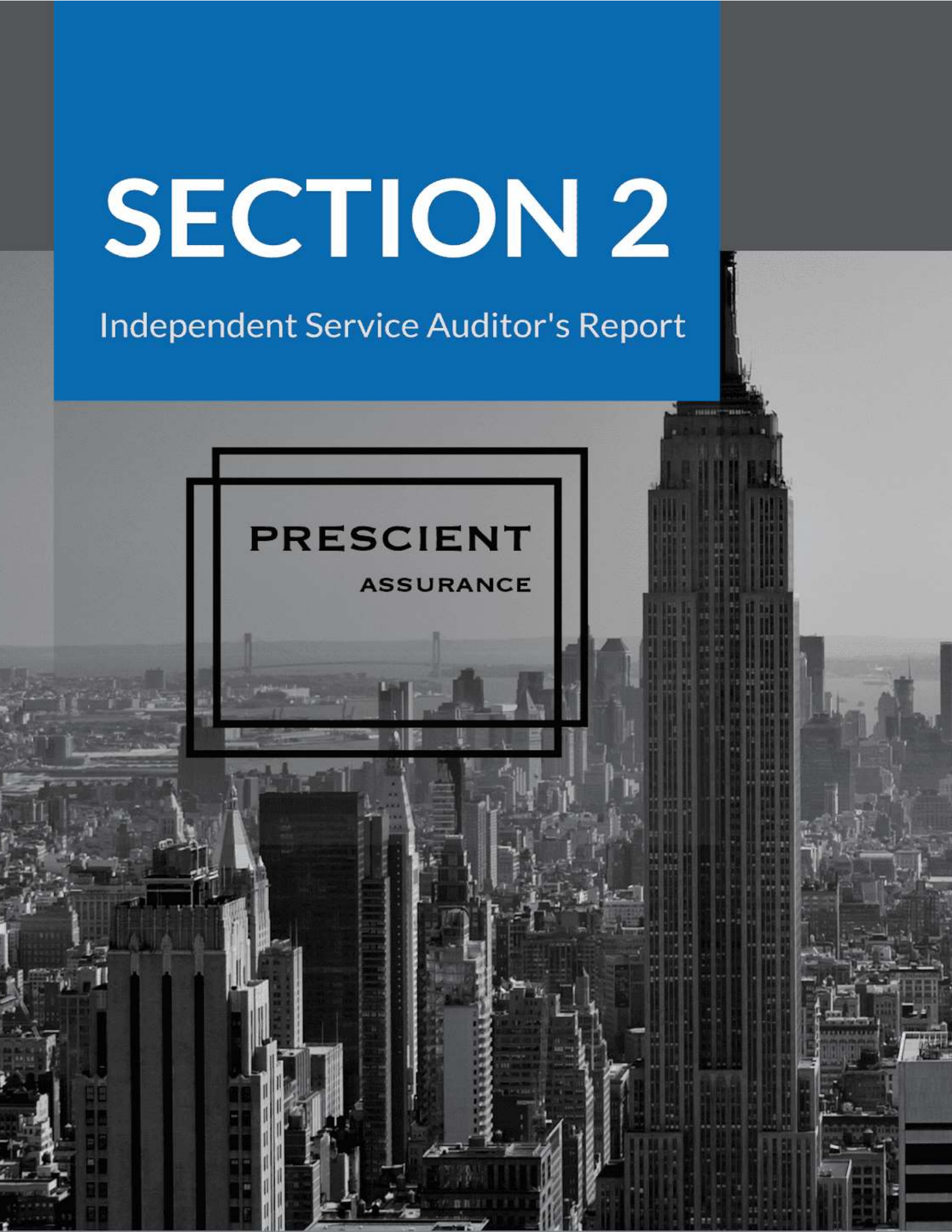
Habib Khan
Controller
0965688 BC LTD



SECTION 2

Independent Service Auditor's Report

PRESCIENT
ASSURANCE



Independent Service Auditor's Report

To: 0965688 BC LTD

Scope

We have examined 0965688 BC LTD's ("0965688 BC LTD") accompanying description of its ProCogia IT Systems system found in Section 3, titled 0965688 BC LTD System Description throughout the period January 1, 2023, to April 15, 2023, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2023, to April 15, 2023, to provide reasonable assurance that 0965688 BC LTD's service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

0965688 BC LTD uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at 0965688 BC LTD, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents 0965688 BC LTD's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of 0965688 BC LTD'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 0965688 BC LTD, to achieve 0965688 BC LTD's service commitments and system requirements based on the applicable trust services criteria. The description presents 0965688 BC LTD's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of 0965688 BC LTD'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 complementary user entity controls.

Service Organization's Responsibilities

0965688 BC LTD 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 0965688 BC LTD's service commitments and system requirements were achieved. In Section 1, 0965688 BC LTD has provided the accompanying assertion titled "Management's Assertion of 0965688 BC LTD" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. 0965688 BC LTD is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.



Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the 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 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:

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

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. 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 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.

Opinion

In our opinion, in all material respects:

- a. The description presents 0965688 BC LTD's system that was designed and implemented throughout the period January 1, 2023, to April 15, 2023, in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period January 1, 2023, to April 15, 2023, to provide reasonable assurance that 0965688 BC LTD's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of 0965688 BC LTD's controls throughout the period.
- c. The controls stated in the description operated effectively throughout the period January 1, 2023, to April 15, 2023, to provide reasonable assurance that 0965688 BC LTD's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of 0965688 BC LTD's controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of 0965688 BC LTD, user entities of 0965688 BC LTD's system during some or all of the period January 1, 2023 to April 15, 2023, business partners of 0965688 BC LTD subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Prescient Assurance LLC

DocuSigned by:
John D Wallace
F5ADFAS569EA450:-----

John D. Wallace, CPA
Chattanooga, TN
May 31, 2023



SECTION 3

System Description



PROCOGIA

DC 1: Company Overview and Types of Products and Services Provided

ProCogia is a market-leading data consultancy fielding a team of agnostic Data experts who deliver end to end Data Solutions to Clients. Our dedicated team helps to deliver on Data Operation, Data Engineering, BI, Analytics and Data Science expertise. These capabilities help to deliver highly scalable data solutions that leverage the full potential of your data. To build agnostic data solutions ProCogia is partnered with AWS, Microsoft, Snowflake & RStudio. We are headquartered in Vancouver, BC with offices in Seattle and Toronto. We work with clients across numerous sectors including Telecom, Pharma, Biotechnology, Retail, Logistics, Technology, Financial Services, Media & non-profit.

DC 2: The Principal Service Commitments and System Requirements

ProCogia adheres to the requirements of our customers (signing of NDAs, adherence of any company policies for sub-contractors).

ProCogia does not store or share any client data, but will operate within client environments.

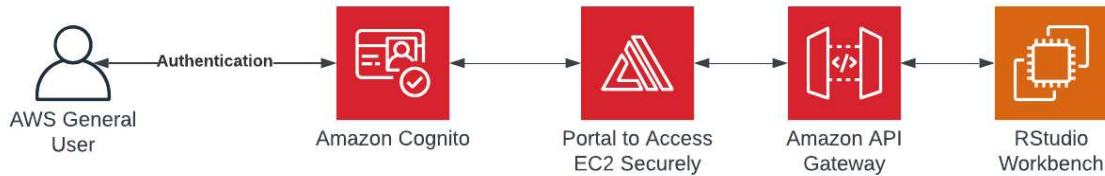
ProCogia enters into Master Service Agreements with customers, defines deliverables via Statements of Work and Level of Effort documents and delivers the agreed upon services to clients in the scope of what is agreed upon.

DC 3: The Components of the System Used to Provide the Services

3.1 Primary Infrastructure

ProCogia predominantly provides services to customers and typically does not maintain any infrastructure around these services.

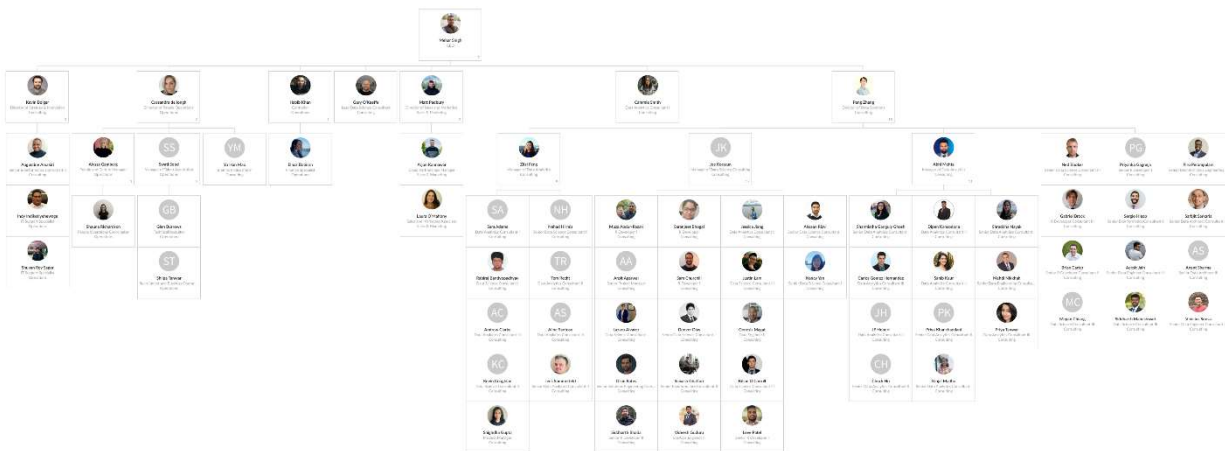
ProCogia does maintain an AWS account for acuna.cloud, where RStudio Teams environment is hosted.



3.2 Primary Software

HubSpot is utilized as a CRM tool. BambooHR is used as a HR management platform. PerformYard is used for performance management. AWS is used to host compute. ClickUp is used to manage project scrum boards to track deliverables. Azure and MS365 are used to manage user accounts. LucidChart is used to develop architectural diagrams.

3.3 People



Leadership Team:

CEO: Mehar Singh

- Reporting in are leadership team

Director of People Operations: Cas de longh

- Reporting in are recruiting and HR

Director of Sales and Marketing: Matthew Padbury

- Reporting in are sales associates & marketing

Director of Data Solutions: Peng Zhang

- Reporting in are consultants and consulting managers.

Controller: Habib Khan

- Reporting in are Finance and IT

3.4 Security Processes and Procedures

ProCogia's Information Security Policy has been developed to: establish a general approach to information security and the minimization of information misuse, compromise or loss; document security processes and measures; uphold ethical standards and meet the company's regulatory, legal, contractual, and other obligations; control business risk; and ensure that the appropriate company image and reputation is presented.

3.5 Data

As a standard practice, ProCogia does not host customer data. In the event that data is potentially requested to be stored within the ProCogia environment, the Data Classification Policy exists as guidance on the labeling and handling of sensitive customer data.

3.6 Third Party Access

The following SaaS platforms host business process data. HubSpot is utilized as a CRM tool. BambooHR is used as a HR management platform. PerformYard is used for performance management. AWS is used to host compute. ClickUp is used to manage project scrum boards to track deliverables. Azure and MS365 are used to manage user accounts. LucidChart is used to develop architectural diagrams. These platforms are controlled and guaranteed by the third party vendors.

3.7 System Boundaries

ProCogia's business processes related to the management of its workforce and management of user profiles and end point machines are in scope.

ProCogia's Acuna Cloud is cloud based managed hosting of RStudio, hosted on an AWS account.

DC 4: Disclosures About Identified Security Incidents

No significant security incidents have occurred during the observation window.

DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved

5.1 Integrity and Ethical Values

ProCogia's Code of Conduct ("Code") is built around our belief that everything we do will be measured against the highest possible standards of ethical business conduct. Our commitment to high standards helps us hire great people, build great products, and attract loyal customers. ProCogia expects all employees to know and follow the Code. Failure to do so can result in disciplinary action, up to and including termination of employment. ProCogia also expects our contractors, consultants, and others who may be temporarily assigned to perform work or services for ProCogia to follow the Code when they work with us. Failure of a ProCogia's contractor, consultant, or other service provider to follow the Code can result in termination of their relationship with ProCogia.

5.2 Commitment to Competence

Employees when they first start at ProCogia go through an orientation from IT and HR where their accounts are set up, then sign any outstanding paperwork and review and accept policies.

5.3 Management's Philosophy and Operating Style

We're a diverse, close-knit team with a common pursuit of providing top-class, end-to-end data solutions for our clients. In return for your talent and technical expertise, you will be rewarded with a competitive salary, generous benefits along with ample opportunity for personal development. 'Growth mindset' is something we seek in all our new hires and has helped drive much of our recent growth across North America. Our distinct approach is to push the limits and value derived from data. Working within ProCogia's thriving environment will allow you to unleash your full career potential.

5.4 Organizational Structure and Assignment of Authority and Responsibility

ProCogia is a data consulting firm. The operational leadership is responsible for the smooth running of support services. The delivery team is responsible for delivering to end clients data solutions. Job descriptions lay out the expectations of individual contributors to serve their customer or provide support services. Leadership job descriptions are constructed to elicit business development and management of employee workforce.

5.5 Human Resource Policies and Practices

Performance of employees is reviewed usually on a quarterly basis using PerformYard performance management platform. Employees are measured on Delivery Quality, Business Growth, Teaching contributions and Learning.

5.6 Security Management

ProCogia has IT Support specialists who manage the day to day operations of the ProCogia IT and Security infrastructure at the direction of the Director of Data & Technology.

5.7 Security and Privacy Policies

- Acceptable Use Policy
- Asset Management Policy
- Backup Policy
- Breach Notification Policy
- Business Associate Policy
- Business Continuity Plan
- Code of Conduct
- Data Classification Policy
- Data Protection Policy
- Data Deletion Policy
- Disaster Recovery Plan
- Encryption Policy
- Incident Response Plan
- Information Security Policy
- Password Policy
- Physical Security Policy
- Privacy, Use, and Disclosure Policy
- Responsible Disclosure Policy
- Risk assessment Policy
- Software Development Lifecycle Policy
- System Access Control Policy
- Vendor management Policy
- Vulnerability Management Policy

5.8 Personnel Security

ProCogia is using the Drata as the compliance automation platform tool. Security awareness training, policy signing and other policies are being assigned and approved in Drata. ProCogia is using Certn as the background check platform. Certn is also connected with Drata and ProCogia can monitor the background check of the employees from that platform.

5.9 Physical Security and Environmental Controls

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

5.10 Change Management

ProCogias policies listed above provide context around how different aspects of the ProCogia ecosystem is managed, maintained and updated.

5.11 System Monitoring

Drata, Azure, AWS and Intune have tools used for system monitoring.

5.12 Incident Management

ProCogia has established the Vulnerability Management Policy to establish the rules for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in the IT environment and the risks associated with them. The ProCogia IT team will facilitate and maintain this policy and ensure all employees review and read the policy. All ProCogia's owned and/or managed Information Resources must use the ProCogia's IT management approved endpoint protection software and configuration. The endpoint protection software must not be altered, bypassed, or disabled. Penetration testing and vulnerability scanning will be conducted at least annually or after any significant changes to the network.

5.13 Data Backup and Recovery

ProCogia maintains backups of key ATS, Finance, HR and CRM Data, separate to the third party applications. In the event of Disaster, the Disaster Recovery Policy exists for guidance.

5.14 System Account Management

Access to ProCogia's systems and applications is limited for all users, including but not limited to workforce members, volunteers, business associates, contracted providers, and consultants. Access by any other entity is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorized use or access of the organization's information systems.

5.15 Risk Management Program

5.15.1 Data Classification

ProCogia's data classification policy will assist employees and other third parties with understanding the Company's information labeling and handling guidelines. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common-sense steps that you can take to protect sensitive or confidential information (e.g., Company Confidential information should not be left

unattended in conference rooms). All the employees of ProCogia are expected to abide by the rules of the data classification policy.

5.15.2 Risk Management Responsibilities

A key element of ProCogia's information security program is a holistic and systematic approach to risk management. The risk assessment policy defines the requirements and processes for ProCogia to

identify information security risks. The process consists of four parts: identification of ProCogia's assets, as well as the threats and vulnerabilities that apply; assessment of the likelihood and consequence (risk) of the threats and vulnerabilities being realized, identification of treatment for each unacceptable risk, and evaluation of the residual risk after treatment.

5.15.3 Risk Management Program Activities

Risk assessment and risk treatment are applied to the entire scope of ProCogia's information security program, and to all assets which are used within ProCogia or which could have an impact on information security within it. This policy applies to all employees of proCogia who take part in risk assessment and risk treatment. ProCogia's information security program is a holistic and systematic approach to risk management. The process consists of four parts: identification of ProCogia's assets, as well as the threats and vulnerabilities that apply; assessment of the likelihood and consequence (risk) of the threats and vulnerabilities being realized, identification of treatment for each unacceptable risk, and evaluation of the residual risk after treatment.

5.15.4 Integration with Risk Assessment

ProCogia takes into account the Impact Levels of an event occurring as well as the likelihood of that event occurring when determining risk to assign it a risk rating.

5.16 Information and Communications Systems

Slack, Teams, Zoom, Sharepoint, Onedrive.

5.17 Data Communication

ProCogia utilizes Nordpass for the secure storage of passwords and keys on endpoint devices.

5.18 Monitoring Controls

ProCogia is using Drata as its compliance automation and monitoring tool. All the policies and control activities such as unique infrastructure, version control and the other platforms are being integrated with the Drata. External assessment such as Pentesting will be done annually and the vulnerability scans quarterly.

DC 6: Complementary User Entity Controls (CUECs)

ProCogia's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to ProCogia's services to be solely achieved by ProCogia's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of ProCogia.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

Trust Services Criteria	Complementary User Entity Controls
CC2.1	User entities are responsible for the security and integrity of data housed under user entity control, particularly the data utilized by ProCogia systems and services.
CC6.2	Determination of personnel who need specific functionality and the granting of such functionality is the responsibility of authorized personnel at the user entity. This includes allowing access to ProCogia's application keys and API keys for access to the web service API
CC6.3	Authorized users and their associated access are reviewed periodically
CC6.6	User entities will ensure protective measures are in place for their data as it traverses from user entity to ProCogia.
CC6.6	User entities should establish adequate physical security and environmental controls of all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity in order to provide authorized information to ProCogia.

DC 7: Complementary Subservice Organization Controls (CSOCs)

Although the subservice organization has been “carved out” for the purposes of this report, certain Trust Services Criteria are intended to be met by controls at the subservice organization.

Complementary Subservice Organization Controls (CSOCs) are expected to be in place at AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities. Management of ProCogia receives and reviews the AWS SOC 2 report annually. In addition, through its operational activities, ProCogia management monitors the services performed by AWS to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to AW management.

It is not feasible for the criteria related to the System to be achieved solely by ProCogia. Therefore, each user entity's internal control must be evaluated in conjunction with ProCogia's controls and related tests, and results described in Section 4 of this report, considering the related CSOCs expected to be implemented at the subservice organization as described below.

Criteria	Complementary Subservice Organization Controls
CC6.4	AWS is responsible for restricting data center access to authorized personnel.
CC6.4	AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC7.2	AWS is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
CC7.2	AWS is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
CC7.2	AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

DC 8: Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant

ProCogia is partially remote and the offices that they do hold are managed by a third party.

DC 9: Disclosures of Significant Changes in Last 1 Year

N/A

SECTION 4

Testing Matrices

**PRESCIENT
ASSURANCE**

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to ProCogia IT Systems provided by 0965688 BC LTD. The scope of the testing was restricted to ProCogia IT Systems, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing throughout the period January 1, 2023 to April 15, 2023.

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

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

Types of Tests Generally Performed

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

Test Types	Description of Tests
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: <ul style="list-style-type: none">• Examination/Inspection of source documentation and authorizations to verify transactions processed.• Examination/Inspection of documents or records for evidence of performance, such as existence of initials or signatures.• Examination/Inspection of systems documentation, configurations, and settings; and



Test Types	Description of Tests
	<ul style="list-style-type: none"> Examination/Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.
Observation	Observed the implementation, application or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Re-performance	Re-performed the control to verify the design and/or operation of the control activity as performed if applicable.

General Sampling Methodology

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Prescient Assurance utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, to determine the number of items to be selected in a sample for a particular test. Prescient Assurance, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

The table below describes the sampling methodology utilized in our testing to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Type of Control and Frequency	Minimum Number of Items to Test (Period of Review Six Months or Less)	Minimum Number of Items to Test (Period of Review More than Six Months)
Manual control, many times per day	At least 25	At least 40
Manual control, daily (Note 1)	At least 25	At least 40
Manual control, weekly	At least 5	At least 10



Type of Control and Frequency	Minimum Number of Items to Test (Period of Review Six Months or Less)	Minimum Number of Items to Test (Period of Review More than Six Months)
Manual control, monthly	At least 3	At least 4
Manual control, quarterly	At least 2	At least 2
Manual control, annually	Test annually	Test annually
Application controls	Test one operation of each relevant aspect of each application control if supported by effective IT general controls; otherwise test at least 15	Test one operation of each application control if supported by effective IT general controls; otherwise test at least 25
IT general controls	Follow guidance above for manual and automated aspects of IT general controls	Follow guidance above for manual and automated aspects of IT general controls

Notes: 1.) Some controls might be performed frequently, but less than daily. For such controls, the sample size should be interpolated using the above guidance. Generally, for controls where the number of occurrences ranges from 50 to 250 during the year, our minimum sample size using the above table should be approximately 10% of the number of occurrences.

Reliability of Information Provided by the Service Organization

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

Test Results

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

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



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



Trust ID	Standard Description	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	ProCogia has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire.	<p>Inspected the personnel data to determine that all employees have accepted the Acceptable Use Policy and that the policy is available to all internal personnel.</p> <p>Inspected the Acceptable Use Policy to determine that the company has established the policies and procedures to guide all employees about the authorized use of company devices, networks, data, and user accounts.</p>	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	ProCogia's new hires are required to pass a background check as a condition of their employment.	<p>Inspected a list of all relevant employees to determine that the company's new hires are required to pass a background check as a condition of their employment.</p> <p>Inspected the Acceptable Use Policy to determine that the company is required to conduct background checks for all new employees and contractors.</p>	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	ProCogia requires its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.	<p>Inspected the personnel data to determine that all contractors have accepted the Code of Conduct and Acceptable Use Policy.</p> <p>Inspected the Code of Conduct and Acceptable Use Policy to determine that the company requires all contractors to follow and accept these policies.</p> <p>Inspected the Acceptable Use Policy to determine that the company requires all contractors to clear a background verification check.</p>	No exceptions noted.
CC1.1	The entity demonstrates a commitment to	ProCogia Management has approved security policies, and all employees accept these	Inspected the personnel data to determine that all current employees have accepted the	No exceptions noted.



	integrity and ethical values.	procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	information security policies and procedures which outline the requirements for securing the company's operations, services, and systems. Observed that all policies have been approved by the management and are accessible to all employees and contractors. Inspected the Information Security Policy, which states that all ISP policies are required to be reviewed, modified, or edited by management, to determine that the company reviews and edits security policies annually.	
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	ProCogia has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	Observed that a Code of Conduct has been published and uploaded on October 25, 2022. Inspected the personnel directory to determine that all employees have accepted the Code of Conduct. Inspected the Code of Conduct to determine that the company has defined the ethical standards that are to be followed by all personnel while performing their duties.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	ProCogia has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.	Inspected the policy acceptance data to determine that the Data Protection Policy has been accepted by all relevant employees and contractors during the observation window. Inspected the Data Protection Policy to determine that the data protection process and encryption methods have been documented.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and	ProCogia has an assigned security team that is responsible for the design, implementation, management, and review of the	Inspected the Organization's Security Policies to determine that the company has reviewed the policies within the last year.	No exceptions noted.



	exercises oversight of the development and performance of internal control.	organization's security policies, standards, baselines, procedures, and guidelines.	Interviewed the company to determine that the Information security and compliance lead is our inhouse specialist responsible for design and implementation of cyber security related policies and procedures.	
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	Inspected the Information Security Policy to determine that the Security & Compliance Lead is responsible for the design, development, maintenance, dissemination, and enforcement of the items contained in all the ISPs.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	ProCogia engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Disclosure: ProCogia does not have a physical network and does not store customer data on its cloud environment, which is why the test has been disabled.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	ProCogia engages with third-party to conduct vulnerability scans of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the vulnerability scan report displaying zero breaches identifies to determine that the company engages with Intruder to conduct vulnerability scans of the production environment. Inspected the Vulnerability Management Policy to determine that the company is required to conduct vulnerability scans of the internal and external network at least annually or after any significant change to the network.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Management reviews security policies on an annual basis.	Inspected the policy list to determine that the Information Security Policy, Acceptable Use Policy, Asset Management Policy, and other security policies have been reviewed in October 2022. Inspected the Information Security Policy to determine that all ISP	No exceptions noted.



			policies must be reviewed, modified, and/or edited annually.	
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the board charter to determine that the roles and responsibilities of the board for providing oversight of the company, monitoring and evaluating the organization's financial performance, and evaluating the performance of the senior management have been defined.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.	Inspected the LinkedIn profile of the company's sole director to determine that the board member is a qualified individual with sufficient expertise to oversee management abilities.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Members of the Board of Directors are independent of management.	Interviewed the company to determine that the Board of Directors are independent of management.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	Inspected the minutes of a board meeting held on November 7, 2022, which included discussions with the senior management to determine that board oversight briefings are held at the company.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.	Inspected the minutes of a meeting of the sole director to determine that the board meets annually to adopt resolutions and oversee the company's performance.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from	ProCogia conducts a Risk Assessment at least annually.	Inspected the risk assessment report which includes the risk assessment approach, their	No exceptions noted.



	management and exercises oversight of the development and performance of internal control.		likelihood, impact level, risk rating, results, treatment plan, and risk register questions to determine that the company performs annual risk assessments. Inspected the Risk Assessment Policy to determine that the company is required to perform a risk assessment at least annually.	
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	ProCogia reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	Inspected the organizational chart of the company, last reviewed on April 18, 2023, and shows the reporting lines and positions of authority to determine that the company has a formal organizational chart in place that is accessible to internal personnel.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	ProCogia has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Organization's Security Policies to determine that the company has reviewed the policies within the last year. Interviewed the company to determine that the Information security and compliance lead is our inhouse specialist responsible for design and implementation of cyber security related policies and procedures.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	ProCogia's new hires are required to pass a background check as a condition of their employment.	Inspected a list of all relevant employees to determine that the company's new hires are required to pass a background check as a condition of their employment. Inspected the Acceptable Use Policy to determine that the company is required to conduct background checks for all new employees and contractors.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in	ProCogia's new hires and/or internal transfers are required to go through an official recruiting process during which their qualifications and experience are screened to ensure that they are	Inspected the Careers page on the company's website which contains current openings with their respective job descriptions to determine that the recruiting process is in place and the hiring	No exceptions noted.



	alignment with objectives.	competent and capable of fulfilling their responsibilities.	manager screens potential candidates for their qualifications and experience to ensure their competency.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	ProCogia evaluates the performance of all employees through a formal, annual performance evaluation.	Inspected a list of employee evaluation and manager evaluation forms showing their completion dates to determine that the company evaluates the performance of all employees through a formal annual performance evaluation.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	All ProCogia positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by ProCogia.	Inspected the Careers page on the company's website, which provides detailed job descriptions of multiple positions, including the required skills, experiences, and responsibilities to determine that ProCogia maintains formal job descriptions for company positions and that the candidates must meet the required criteria to get hired.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	ProCogia has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with ProCogia's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	Inspected a Drata security training certificate of an employee to determine that employees complete annual security awareness training within Drata. Inspected the Information Security Policy to determine that all new hires are required to complete information security awareness training as part of their new employee onboarding process and annually thereafter.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	ProCogia has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	Observed that a Code of Conduct has been published and uploaded on October 25, 2022. Inspected the personnel directory to determine that all employees have accepted the Code of Conduct. Inspected the Code of Conduct to determine that the company has	No exceptions noted.



			defined the ethical standards that are to be followed by all personnel while performing their duties.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	ProCogia requires its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.	<p>Inspected the personnel data to determine that all contractors have accepted the Code of Conduct and Acceptable Use Policy.</p> <p>Inspected the Code of Conduct and Acceptable Use Policy to determine that the company requires all contractors to follow and accept these policies.</p> <p>Inspected the Acceptable Use Policy to determine that the company requires all contractors to clear a background verification check.</p>	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	ProCogia has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	<p>Observed that a Code of Conduct has been published and uploaded on October 25, 2022.</p> <p>Inspected the personnel directory to determine that all employees have accepted the Code of Conduct.</p> <p>Inspected the Code of Conduct to determine that the company has defined the ethical standards that are to be followed by all personnel while performing their duties.</p>	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	ProCogia has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with ProCogia's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	<p>Inspected a Drata security training certificate of an employee to determine that employees complete annual security awareness training within Drata.</p> <p>Inspected the Information Security Policy to determine that all new hires are required to complete information security awareness training as part of their new employee onboarding process and annually thereafter.</p>	No exceptions noted.



CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	ProCogia has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire.	<p>Inspected the personnel data to determine that all employees have accepted the Acceptable Use Policy and that the policy is available to all internal personnel.</p> <p>Inspected the Acceptable Use Policy to determine that the company has established the policies and procedures to guide all employees about the authorized use of company devices, networks, data, and user accounts.</p>	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	ProCogia evaluates the performance of all employees through a formal, annual performance evaluation.	Inspected a list of employee evaluation and manager evaluation forms showing their completion dates to determine that the company evaluates the performance of all employees through a formal annual performance evaluation.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	ProCogia Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.	<p>Inspected the Acceptable Use Policy, Asset Management Policy, Data Protection Policy, Information Security Policy, and other policies to determine that relevant policies that detail how customer data may be accessed and handled have been approved by the management and are accessible to all employees and contractors.</p> <p>Inspected the Data Protection Policy to determine that customer data access, monitoring, and protection processes have been described.</p>	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	ProCogia has an established policy and procedures that governs the use of cryptographic controls.	Inspected the Encryption Policy to determine that the company has established the cryptographic controls and procedures for cryptographic key management and protection.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality	ProCogia performs control self-assessments at least annually to gain assurance that controls	Inspected the control test results in Drata to determine that the	No exceptions noted.



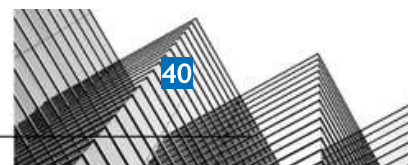
	information to support the functioning of internal control.	are in place and operating effectively. Corrective actions are taken based on relevant findings.	company performs self-assessments via Drata.	
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	ProCogia conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Observed that the company uses Drata to perform continuous monitoring of its information controls.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	ProCogia conducts a Risk Assessment at least annually.	Inspected the risk assessment report which includes the risk assessment approach, their likelihood, impact level, risk rating, results, treatment plan, and risk register questions to determine that the company performs annual risk assessments. Inspected the Risk Assessment Policy to determine that the company is required to perform a risk assessment at least annually.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	ProCogia has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Inspected the Information Security Policy to determine that an Information Security Policy is in place stating the requirements and general approaches for information security controls and compliance.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	ProCogia authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.	Observed Role Based Settings and Integrations to determine the company's resources are based on the principle of least privilege. Inspected the System Access Control Policy to determine that the company grants users access to company systems and applications based on the principle of least privilege.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	ProCogia identifies, inventories and classifies virtualized assets.	Inspected the asset inventory to determine that the company maintains a record of all its assets including asset classification, owners, and descriptions. Inspected the Asset Management	No exceptions noted.



			Policy to determine that the company has documented the standards for maintaining an asset inventory for physical and virtual assets.	
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	ProCogia maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control.	<p>Inspected the architectural diagrams of the company to determine that the boundaries of the system and the workflow of traffic have been defined and documented.</p> <p>Inspected the Asset Management Policy to determine that the company is required to maintain an accurate and updated network diagram.</p>	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.	ProCogia has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.	<p>Inspected the policy acceptance data to determine that the Data Protection Policy has been accepted by all relevant employees and contractors during the observation window.</p> <p>Inspected the Data Protection Policy to determine that the data protection process and encryption methods have been documented.</p>	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.	ProCogia provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.	Inspected the Responsible Disclosure Policy to determine that an email address (vulnerability@procogia.com) has been provided to employees to submit a vulnerability report to the Product Security Team.	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.	ProCogia has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-ups to completion.	Inspected the Incident Response Plan to determine that the company has defined the incident response process, which requires conducting a post-mortem that includes root cause analysis and documentation of any lessons learned.	No exceptions noted.



			Disclosure: No security incidents occurred during the observation window.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	ProCogia has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.	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.	ProCogia conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Observed that the company uses Drata to perform continuous monitoring of its information controls.	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.	ProCogia Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	<p>Inspected the personnel data to determine that all current employees have accepted the information security policies and procedures which outline the requirements for securing the company's operations, services, and systems.</p> <p>Observed that all policies have been approved by the management and are accessible to all employees and contractors.</p> <p>Inspected the Information Security Policy, which states that all ISP policies are required to be reviewed, modified, or edited by management, to determine that the company reviews and edits security policies annually.</p>	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.	The security team communicates important information security events to company management in a timely manner.	<p>Inspected the Incident Response Plan to determine that when an information security incident is identified or detected, users are required to notify their immediate manager within 24 hours and the manager should immediately notify the ISM on call for a proper response.</p> <p>Disclosure: No security incidents occurred during the observation window.</p>	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.	ProCogia has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with ProCogia's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	<p>Inspected a Drata security training certificate of an employee to determine that employees complete annual security awareness training within Drata.</p> <p>Inspected the Information Security Policy to determine that all new hires are required to complete information security awareness training as part of their new employee onboarding process and annually thereafter.</p>	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.	ProCogia has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	<p>Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.</p> <p>Disclosure: No security incidents occurred during the observation window.</p>	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support	ProCogia has implemented an Incident Response Policy that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team.	Inspected the Incident Response Plan to determine that the company requires the ISM to conduct a post-mortem after an incident has been resolved that includes root cause analysis and documentation of any lessons	No exceptions noted.



	the functioning of internal control.		learned. Disclosure: No security incidents occurred during the observation window.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	ProCogia has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	Observed that a Code of Conduct has been published and uploaded on October 25, 2022. Inspected the personnel directory to determine that all employees have accepted the Code of Conduct. Inspected the Code of Conduct to determine that the company has defined the ethical standards that are to be followed by all personnel while performing their duties.	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.	ProCogia has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire.	Inspected the personnel data to determine that all employees have accepted the Acceptable Use Policy and that the policy is available to all internal personnel. Inspected the Acceptable Use Policy to determine that the company has established the policies and procedures to guide all employees about the authorized use of company devices, networks, data, and user accounts.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	ProCogia has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents. Disclosure: No security incidents occurred during the observation window.	No exceptions noted.
CC2.3	The entity communicates with	ProCogia maintains a Privacy Policy that is available to all	Inspected the Privacy Policy on the company's website to determine	No exceptions noted.



	external parties regarding matters affecting the functioning of internal control.	external users and internal employees, and it details the company's confidentiality and privacy commitments.	that the company has made its privacy and security commitments accessible to all internal and external users through its website.	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	ProCogia maintains a Terms of Service that is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems. Client Agreements or Master Service Agreements are in place for when the Terms of Service may not apply.	Inspected a signed MSA to determine that service commitments are communicated to all external users.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	ProCogia provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.	Inspected the company's website to determine that the company has provided a contact form for external users to report complaints and other concerns.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	ProCogia maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	<p>Inspected the vendor directory which includes a list of vendors along with their categories, risk levels, owners, and links to their Privacy Policy and Terms of Use to determine that the company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.</p> <p>Inspected High Risk Compliance reports to determine that the company's critical vendor compliance reports are reviewed annually.</p> <p>Inspected the Vendor Management Policy to determine that the company may choose to audit IT vendors and partners to ensure compliance with applicable security policies, as well as legal, regulatory and contractual</p>	No exceptions noted.



			obligations.	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	ProCogia tracks security deficiencies through internal tools and closes them within an SLA that management has pre-specified.	<p>Inspected the Incident Response Plan to determine that the company has defined the incident response process, which requires conducting a post-mortem that includes root cause analysis and documentation of any lessons learned.</p> <p>Disclosure: No security incidents occurred during the observation window.</p>	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	ProCogia has implemented an Incident Response Policy that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team.	<p>Inspected the Incident Response Plan to determine that the company requires the ISM to conduct a post-mortem after an incident has been resolved that includes root cause analysis and documentation of any lessons learned.</p> <p>Disclosure: No security incidents occurred during the observation window.</p>	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	ProCogia has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-ups to completion.	<p>Inspected the Incident Response Plan to determine that the company has defined the incident response process, which requires conducting a post-mortem that includes root cause analysis and documentation of any lessons learned.</p> <p>Disclosure: No security incidents occurred during the observation window.</p>	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	ProCogia maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the vendor directory which includes a list of vendors along with their categories, risk levels, owners, and links to their Privacy Policy and Terms of Use to determine that the company maintains a directory of its key vendors, including its agreements that specify terms, conditions and	No exceptions noted.



			responsibilities. Inspected the Vendor Management Policy which details the requirements for maintaining a vendor inventory and vendor contracts that must include confidentiality and privacy commitments, to determine that the company is required to maintain a directory of its key vendors, including its agreements that specify terms, conditions, and responsibilities.	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	ProCogia has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	ProCogia's security commitments are communicated to external users, as appropriate.	Inspected the Cookie Policy and Privacy Policy to determine that the company's security commitments are communicated to external users through its website.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	ProCogia engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Disclosure: ProCogia does not have a physical network and does not store customer data on its cloud environment, which is why the test has been disabled.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	ProCogia 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.	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for identified risks based on their severity levels.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the	ProCogia conducts a Risk Assessment at least annually.	Inspected the risk assessment report which includes the risk assessment approach, their likelihood, impact level, risk	No exceptions noted.



	identification and assessment of risks relating to objectives.		rating, results, treatment plan, and risk register questions to determine that the company performs annual risk assessments. Inspected the Risk Assessment Policy to determine that the company is required to perform a risk assessment at least annually.	
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	ProCogia engages with third-party to conduct vulnerability scans of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the vulnerability scan report displaying zero breaches identifies to determine that the company engages with Intruder to conduct vulnerability scans of the production environment. Inspected the Vulnerability Management Policy to determine that the company is required to conduct vulnerability scans of the internal and external network at least annually or after any significant change to the network.	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.	ProCogia maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inspected the vendor directory which includes a list of vendors along with their categories, risk levels, owners, and links to their Privacy Policy and Terms of Use to determine that the company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities. Inspected High Risk Compliance reports to determine that the company's critical vendor compliance reports are reviewed annually. Inspected the Vendor Management Policy to determine that the company may choose to audit IT vendors and partners to ensure compliance with applicable security policies, as well as legal,	No exceptions noted.



			regulatory and contractual obligations.	
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.	ProCogia's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	<p>Inspected the Risk Assessment report which contains a risk treatment plan for identified vulnerabilities to determine that the company has prepared a remediation plan.</p> <p>Inspected the Risk Assessment Policy to determine that the company has established a risk remediation process that is required to be implemented to resolve any incidents.</p>	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.	ProCogia 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.	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for identified risks based on their severity levels.	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.	ProCogia engages with third-party to conduct vulnerability scans of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	<p>Inspected the vulnerability scan report displaying zero breaches identifies to determine that the company engages with Intruder to conduct vulnerability scans of the production environment.</p> <p>Inspected the Vulnerability Management Policy to determine that the company is required to conduct vulnerability scans of the internal and external network at least annually or after any significant change to the network.</p>	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.	ProCogia conducts a Risk Assessment at least annually.	Inspected the risk assessment report which includes the risk assessment approach, their likelihood, impact level, risk rating, results, treatment plan, and risk register questions to determine that the company performs annual risk assessments.	No exceptions noted.



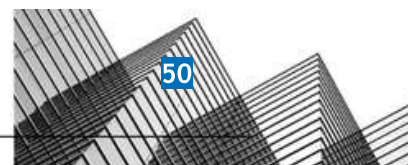
			Inspected the Risk Assessment Policy to determine that the company is required to perform a risk assessment at least annually.	
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	ProCogia maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	<p>Inspected the vendor directory which includes a list of vendors along with their categories, risk levels, owners, and links to their Privacy Policy and Terms of Use to determine that the company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.</p> <p>Inspected the Vendor Management Policy which details the requirements for maintaining a vendor inventory and vendor contracts that must include confidentiality and privacy commitments, to determine that the company is required to maintain a directory of its key vendors, including its agreements that specify terms, conditions, and responsibilities.</p>	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	ProCogia conducts a Risk Assessment at least annually.	<p>Inspected the risk assessment report which includes the risk assessment approach, their likelihood, impact level, risk rating, results, treatment plan, and risk register questions to determine that the company performs annual risk assessments.</p> <p>Inspected the Risk Assessment Policy to determine that the company is required to perform a risk assessment at least annually.</p>	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	ProCogia's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the Risk Assessment report which contains a risk treatment plan for identified vulnerabilities to determine that the company has prepared a remediation plan.	No exceptions noted.



			Inspected the Risk Assessment Policy to determine that the company has established a risk remediation process that is required to be implemented to resolve any incidents.	
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	ProCogia conducts a Risk Assessment at least annually.	<p>Inspected the risk assessment report which includes the risk assessment approach, their likelihood, impact level, risk rating, results, treatment plan, and risk register questions to determine that the company performs annual risk assessments.</p> <p>Inspected the Risk Assessment Policy to determine that the company is required to perform a risk assessment at least annually.</p>	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	ProCogia maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	<p>Inspected the vendor directory which includes a list of vendors along with their categories, risk levels, owners, and links to their Privacy Policy and Terms of Use to determine that the company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.</p> <p>Inspected the Vendor Management Policy which details the requirements for maintaining a vendor inventory and vendor contracts that must include confidentiality and privacy commitments, to determine that the company is required to maintain a directory of its key vendors, including its agreements that specify terms, conditions, and responsibilities.</p>	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	ProCogia reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of	Inspected the organizational chart of the company, last reviewed on April 18, 2023, and shows the reporting lines and positions of authority to determine that the	No exceptions noted.



		information security on an annual basis.	company has a formal organizational chart in place that is accessible to internal personnel.	
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	ProCogia engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Disclosure: ProCogia does not have a physical network and does not store customer data on its cloud environment.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	ProCogia engages with third-party to conduct vulnerability scans of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the vulnerability scan report displaying zero breaches identifies to determine that the company engages with Intruder to conduct vulnerability scans of the production environment. Inspected the Vulnerability Management Policy to determine that the company is required to conduct vulnerability scans of the internal and external network at least annually or after any significant change to the network.	No exceptions noted.
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.	ProCogia performs annual access control reviews.	Inspected the blocked status of an inactive account to determine that the company performs access control reviews and changes the access levels when required. Inspected an email with the distribution list and list of members attached to determine that the company performs annual access control reviews. Inspected the System Access Control Policy to determine that the company is required to perform annual access control reviews.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal	ProCogia maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the vendor directory which includes a list of vendors along with their categories, risk levels, owners, and links to their Privacy Policy and Terms of Use to determine that the company	No exceptions noted.



	control are present and functioning.		<p>maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.</p> <p>Inspected the Vendor Management Policy which details the requirements for maintaining a vendor inventory and vendor contracts that must include confidentiality and privacy commitments, to determine that the company is required to maintain a directory of its key vendors, including its agreements that specify terms, conditions, and responsibilities.</p>	
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.	ProCogia has a defined System Access Control Policy that requires annual access control reviews to be conducted and access request forms be filled out for new hires and employee transfers.	Inspected the System Access Control Policy to determine that all access to the company's systems and services is reviewed and updated on an annual basis to ensure proper authorizations are in place commensurate with job functions.	No exceptions noted.
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.	ProCogia conducts a Risk Assessment at least annually.	<p>Inspected the risk assessment report which includes the risk assessment approach, their likelihood, impact level, risk rating, results, treatment plan, and risk register questions to determine that the company performs annual risk assessments.</p> <p>Inspected the Risk Assessment Policy to determine that the company is required to perform a risk assessment at least annually.</p>	No exceptions noted.
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.	ProCogia engages with third-party to conduct vulnerability scans of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	<p>Inspected the vulnerability scan report displaying zero breaches identifies to determine that the company engages with Intruder to conduct vulnerability scans of the production environment.</p> <p>Inspected the Vulnerability Management Policy to determine</p>	No exceptions noted.



			that the company is required to conduct vulnerability scans of the internal and external network at least annually or after any significant change to the network.	
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.	ProCogia engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Disclosure: ProCogia does not have a physical network and does not store customer data on its cloud environment.	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.	ProCogia has implemented an Incident Response Policy that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team.	Inspected the Incident Response Plan to determine that the company requires the ISM to conduct a post-mortem after an incident has been resolved that includes root cause analysis and documentation of any lessons learned. Disclosure: No security incidents occurred during the observation window.	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.	ProCogia engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Disclosure: ProCogia does not have a physical network and does not store customer data on its cloud environment.	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.	ProCogia's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the Risk Assessment report which contains a risk treatment plan for identified vulnerabilities to determine that the company has prepared a remediation plan. Inspected the Risk Assessment Policy to determine that the company has established a risk remediation process that is	No exceptions noted.



			required to be implemented to resolve any incidents.	
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.	ProCogia engages with third-party to conduct vulnerability scans of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the vulnerability scan report displaying zero breaches identifies to determine that the company engages with Intruder to conduct vulnerability scans of the production environment. Inspected the Vulnerability Management Policy to determine that the company is required to conduct vulnerability scans of the internal and external network at least annually or after any significant change to the network.	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.	ProCogia has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.	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.	ProCogia has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Organization's Security Policies to determine that the company has reviewed the policies within the last year. Interviewed the company to determine that the Information security and compliance lead is our inhouse specialist responsible for design and implementation of cyber security related policies and procedures.	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	ProCogia has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.	No exceptions noted.



	management and the board of directors, as appropriate.		Disclosure: No security incidents occurred during the observation window.	
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.	ProCogia conducts a Risk Assessment at least annually.	Inspected the risk assessment report which includes the risk assessment approach, their likelihood, impact level, risk rating, results, treatment plan, and risk register questions to determine that the company performs annual risk assessments. Inspected the Risk Assessment Policy to determine that the company is required to perform a risk assessment at least annually.	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.	ProCogia has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-ups to completion.	Inspected the Incident Response Plan to determine that the company has defined the incident response process, which requires conducting a post-mortem that includes root cause analysis and documentation of any lessons learned. Disclosure: No security incidents occurred during the observation window.	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.	ProCogia maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the vendor directory which includes a list of vendors along with their categories, risk levels, owners, and links to their Privacy Policy and Terms of Use to determine that the company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities. Inspected the Vendor Management Policy which details the requirements for maintaining a vendor inventory and vendor contracts that must include confidentiality and privacy commitments, to determine that	No exceptions noted.



			the company is required to maintain a directory of its key vendors, including its agreements that specify terms, conditions, and responsibilities.	
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	ProCogia engages with third-party to conduct vulnerability scans of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	<p>Inspected the vulnerability scan report displaying zero breaches identifies to determine that the company engages with Intruder to conduct vulnerability scans of the production environment.</p> <p>Inspected the Vulnerability Management Policy to determine that the company is required to conduct vulnerability scans of the internal and external network at least annually or after any significant change to the network.</p>	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	ProCogia engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Disclosure: ProCogia does not have a physical network and does not store customer data on its cloud environment.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	ProCogia has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	<p>Inspected the Organization's Security Policies to determine that the company has reviewed the policies within the last year.</p> <p>Interviewed the company to determine that the Information security and compliance lead is our inhouse specialist responsible for design and implementation of cyber security related policies and procedures.</p>	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	ProCogia conducts a Risk Assessment at least annually.	Inspected the risk assessment report which includes the risk assessment approach, their likelihood, impact level, risk rating, results, treatment plan, and risk register questions to determine that the company performs annual risk assessments.	No exceptions noted.



			Inspected the Risk Assessment Policy to determine that the company is required to perform a risk assessment at least annually.	
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	ProCogia 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.	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for identified risks based on their severity levels.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	ProCogia's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the Risk Assessment report which contains a risk treatment plan for identified vulnerabilities to determine that the company has prepared a remediation plan. Inspected the Risk Assessment Policy to determine that the company has established a risk remediation process that is required to be implemented to resolve any incidents.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	ProCogia reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	Inspected the organizational chart of the company, last reviewed on April 18, 2023, and shows the reporting lines and positions of authority to determine that the company has a formal organizational chart in place that is accessible to internal personnel.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	ProCogia conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Observed that the company uses Drata to perform continuous monitoring of its information controls.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support	ProCogia Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are	Inspected the Acceptable Use Policy, Asset Management Policy, Data Protection Policy, Information Security Policy, and other policies to determine that relevant	No exceptions noted.



	the achievement of objectives.	accessible to all employees and contractors.	<p>policies that detail how customer data may be accessed and handled have been approved by the management and are accessible to all employees and contractors.</p> <p>Inspected the Data Protection Policy to determine that customer data access, monitoring, and protection processes have been described.</p>	
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	ProCogia engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Disclosure: ProCogia does not have a physical network and does not store customer data on its cloud environment.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	ProCogia has an established policy and procedures that governs the use of cryptographic controls.	Inspected the Encryption Policy to determine that the company has established the cryptographic controls and procedures for cryptographic key management and protection.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	ProCogia conducts a Risk Assessment at least annually.	<p>Inspected the risk assessment report which includes the risk assessment approach, their likelihood, impact level, risk rating, results, treatment plan, and risk register questions to determine that the company performs annual risk assessments.</p> <p>Inspected the Risk Assessment Policy to determine that the company is required to perform a risk assessment at least annually.</p>	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	ProCogia engages with third-party to conduct vulnerability scans of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	<p>Inspected the vulnerability scan report displaying zero breaches identifies to determine that the company engages with Intruder to conduct vulnerability scans of the production environment.</p> <p>Inspected the Vulnerability Management Policy to determine that the company is required to</p>	No exceptions noted.



			conduct vulnerability scans of the internal and external network at least annually or after any significant change to the network.	
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	ProCogia authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.	Observed Role Based Settings and Integrations to determine the company's resources are based on the principle of least privilege. Inspected the System Access Control Policy to determine that the company grants users access to company systems and applications based on the principle of least privilege.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	ProCogia conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Observed that the company uses Drata to perform continuous monitoring of its information controls.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	ProCogia's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the Risk Assessment report which contains a risk treatment plan for identified vulnerabilities to determine that the company has prepared a remediation plan. Inspected the Risk Assessment Policy to determine that the company has established a risk remediation process that is required to be implemented to resolve any incidents.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	ProCogia has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Organization's Security Policies to determine that the company has reviewed the policies within the last year. Interviewed the company to determine that the Information security and compliance lead is our inhouse specialist responsible for design and implementation of cyber security related policies and procedures.	No exceptions noted.



CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	ProCogia Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	<p>Inspected the personnel data to determine that all current employees have accepted the information security policies and procedures which outline the requirements for securing the company's operations, services, and systems.</p> <p>Observed that all policies have been approved by the management and are accessible to all employees and contractors.</p> <p>Inspected the Information Security Policy, which states that all ISP policies are required to be reviewed, modified, or edited by management, to determine that the company reviews and edits security policies annually.</p>	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	ProCogia has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with ProCogia's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	<p>Inspected a Drata security training certificate of an employee to determine that employees complete annual security awareness training within Drata.</p> <p>Inspected the Information Security Policy to determine that all new hires are required to complete information security awareness training as part of their new employee onboarding process and annually thereafter.</p>	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.	ProCogia has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	<p>Observed that a Code of Conduct has been published and uploaded on October 25, 2022.</p> <p>Inspected the personnel directory to determine that all employees have accepted the Code of Conduct.</p> <p>Inspected the Code of Conduct to determine that the company has defined the ethical standards that</p>	No exceptions noted.



			are to be followed by all personnel while performing their duties.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	ProCogia 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.	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for identified risks based on their severity levels.	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.	ProCogia provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.	Inspected the Responsible Disclosure Policy to determine that an email address (vulnerability@procogia.com) has been provided to employees to submit a vulnerability report to the Product Security Team.	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.	ProCogia has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Disaster Recovery Plan to determine that the disaster recovery procedure and the roles and responsibilities of the Security Officer for the implementation of recovery procedures have been defined by the company.	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.	ProCogia conducts annual BCP/DR tests and documents according to the BCDR Plan.	<p>Inspected the tabletop exercises which include test scenarios, discussions, and steps for analyzing and mitigating the issue to determine that the company performs annual disaster recovery tests.</p> <p>Inspected the Business Continuity Plan and the Disaster Recovery Plan to determine that the company is required to simulate and test these plans at least annually through tabletop and technical testing.</p>	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.	ProCogia has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Inspected the Information Security Policy to determine that an Information Security Policy is in place stating the requirements and general approaches for information security controls and compliance.	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.	ProCogia Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	<p>Inspected the personnel data to determine that all current employees have accepted the information security policies and procedures which outline the requirements for securing the company's operations, services, and systems.</p> <p>Observed that all policies have been approved by the management and are accessible to all employees and contractors.</p> <p>Inspected the Information Security Policy, which states that all ISP policies are required to be reviewed, modified, or edited by management, to determine that the company reviews and edits security policies annually.</p>	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.	Management reviews security policies on an annual basis.	<p>Inspected the policy list to determine that the Information Security Policy, Acceptable Use Policy, Asset Management Policy, and other security policies have been reviewed in October 2022.</p> <p>Inspected the Information Security Policy to determine that all ISP policies must be reviewed, modified, and/or edited annually.</p>	No exceptions noted.
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.	ProCogia requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.	<p>Observed that MFA is enabled on all employees' identity provider accounts.</p> <p>Inspected the Password Policy to determine that the company requires MFA to be enabled for all systems that provide the option for MFA.</p>	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over	Appropriate levels of access to infrastructure tools are granted.	Observed Access Request Email to determine that the company grants appropriate levels of access to infrastructure tools.	No exceptions noted.



	protected information assets to protect them from security events to meet the entity's objectives.		Inspected the System Access Control Policy to determine that the Security Officer is required to grant or reject access to systems as dictated by the employee's role and job title and/or as needed.	
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.	ProCogia maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.	<p>Inspected the architecture diagram, last reviewed on November 9, 2022, showing the service architecture and used applications to determine that the company maintains an accurate and current network diagram.</p> <p>Inspected the Asset Management Policy to determine that a network diagram is available to all appropriate service personnel and is kept current.</p>	No exceptions noted.
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.	ProCogia has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	Inspected the Password Policy to determine that formal guidelines and requirements regarding password length and complexity have been established by the management.	No exceptions noted.
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.	ProCogia has an established key management process in place to support the organization's use of cryptographic techniques.	Inspected the Encryption Policy to determine that the company has described a key management system to guide the workforce in the use of public and private encryption keys.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to	ProCogia uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	<p>Observed that the company uses GitHub as a version control system. However, it is used only for testing purposes currently.</p> <p>Inspected the Software Development Policy which states the design system components</p>	No exceptions noted.



	meet the entity's objectives.		phase transforms requirements into specifications to guide the work of the development phase to determine that the company uses a version control system to manage source code, documentation, release labeling, and other change management tasks.	
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.	Hardening standards are in place to ensure that newly deployed server instances are appropriately secured.	Observed that the company uses AWS as its infrastructure provider, which has industry-level hardening standards. Inspected the Asset Management Policy to determine that the company requires manufacturer-provided hardening and best practice guides to be employed to ensure that all devices are properly guarded against vulnerabilities and unauthorized access attempts.	No exceptions noted.
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.	ProCogia ensures that a password manager is installed on all company-issued laptops.	Inspected the personnel data to determine that all employees have a password manager installed on their workstations. Inspected the Password Policy to determine that the company requires all its employees to use an approved password manager NordPass, and any modern, up-to-date browser to store passwords electronically.	No exceptions noted.
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.	ProCogia identifies, inventories and classifies virtualized assets.	Inspected the asset inventory to determine that the company maintains a record of all its assets including asset classification, owners, and descriptions. Inspected the Asset Management Policy to determine that the company has documented the standards for maintaining an asset inventory for physical and virtual assets.	No exceptions noted.



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.	ProCogia ensures that company-issued laptops have encrypted hard-disks.	<p>Inspected the personnel data displaying that all employees have hard disk encryption enabled on their workstations to determine that all company-issued laptops have encrypted hard disks.</p> <p>Inspected the System Access Control Policy to determine that the company requires hard drives to be encrypted.</p>	No exceptions noted.
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.	Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for external users, and MFA required for employee users.	<p>Inspected the authentication settings showing a contact number that is used for verification upon signing in to determine that authentication is required before access is granted.</p> <p>Inspected the personnel data to determine that all current employees and contractors have identity MFA enabled and have unique email IDs.</p> <p>Inspected the Password Policy to determine that the company requires strong passwords to be used and MFA to be enabled for all systems that provide the option for it.</p>	No exceptions noted.
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.	Role-based security is in place for internal and external users, including super admin users.	<p>Observed Global Administrator settings to determine that the company has Role-based security in place.</p> <p>Inspected the System Access Control Policy to determine that the company requires users to be granted access to the organization's information systems based on their job responsibilities.</p>	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information	Access to corporate networks, production machines, network devices, and support tools requires a unique ID.	Inspected the personnel data to determine that all employees have been assigned unique email accounts to access the corporate network.	No exceptions noted.



	assets to protect them from security events to meet the entity's objectives.		Inspected the Password Policy which states the password and MFA requirements for accessing the company's network and systems, to determine that access to the corporate network, production machines, network devices, and support tools requires a unique ID.	
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Access to infrastructure and code review tools is removed from terminated employees within one business day.	Inspected System Access Control Policy to determine that the Security Officer is required to terminate users' access rights within 1 business day of termination/separation.	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.	Access to corporate networks, production machines, network devices, and support tools requires a unique ID.	<p>Inspected the personnel data to determine that all employees have been assigned unique email accounts to access the corporate network.</p> <p>Inspected the Password Policy which states the password and MFA requirements for accessing the company's network and systems, to determine that access to the corporate network, production machines, network devices, and support tools requires a unique ID.</p>	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and	ProCogia has a defined System Access Control Policy that requires annual access control reviews to be conducted and access request forms be filled out	Inspected the System Access Control Policy to determine that all access to the company's systems and services is reviewed and updated on an annual basis to	No exceptions noted.



	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.	for new hires and employee transfers.	ensure proper authorizations are in place commensurate with job functions.	
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.	A termination checklist is used to ensure that system access, including physical access, for terminated employees has been removed within one specified time	Inspected the System Access Control Policy to determine that the HR department, users, and their supervisors are required to notify the Security Officer upon completion and/or termination of access needs and facilitate completion of the termination checklist. Disclosure: No employees were terminated during the observation window.	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.	ProCogia performs annual access control reviews.	Inspected the blocked status of an inactive account to determine that the company performs access control reviews and changes the access levels when required. Inspected an email with the distribution list and list of members attached to determine that the company performs annual access control reviews. Inspected the System Access Control Policy to determine that the company is required to perform annual access control reviews.	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.	Appropriate levels of access to infrastructure tools are granted.	Observed Access Request Email to determine that the company grants appropriate levels of access to infrastructure tools. Inspected the System Access Control Policy to determine that the Security Officer is required to grant or reject access to systems as dictated by the employee's role and job title and/or as needed.	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.	A termination checklist is used to ensure that system access, including physical access, for terminated employees has been removed within one specified time	Inspected the System Access Control Policy to determine that the HR department, users, and their supervisors are required to notify the Security Officer upon completion and/or termination of access needs and facilitate completion of the termination checklist. Disclosure: No employees were terminated during the observation window.	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,	Access to infrastructure and code review tools is removed from terminated employees within one business day.	Inspected System Access Control Policy to determine that the Security Officer is required to terminate users' access rights within 1 business day of termination/separation.	No exceptions noted.



	to meet the entity's objectives.			
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.	ProCogia performs annual access control reviews.	<p>Inspected the blocked status of an inactive account to determine that the company performs access control reviews and changes the access levels when required.</p> <p>Inspected an email with the distribution list and list of members attached to determine that the company performs annual access control reviews.</p> <p>Inspected the System Access Control Policy to determine that the company is required to perform annual access control reviews.</p>	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.	Role-based security is in place for internal and external users, including super admin users.	<p>Observed Global Administrator settings to determine that the company has Role-based security in place.</p> <p>Inspected the System Access Control Policy to determine that the company requires users to be granted access to the organization's information systems based on their job responsibilities.</p>	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.	ProCogia has a defined System Access Control Policy that requires annual access control reviews to be conducted and access request forms be filled out for new hires and employee transfers.	Inspected the System Access Control Policy to determine that all access to the company's systems and services is reviewed and updated on an annual basis to ensure proper authorizations are in place commensurate with job functions.	No exceptions noted.



	privilege and segregation of duties, to meet the entity's objectives.			
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Access to corporate networks, production machines, network devices, and support tools requires a unique ID.	<p>Inspected the personnel data to determine that all employees have been assigned unique email accounts to access the corporate network.</p> <p>Inspected the Password Policy which states the password and MFA requirements for accessing the company's network and systems, to determine that access to the corporate network, production machines, network devices, and support tools requires a unique ID.</p>	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.	Appropriate levels of access to infrastructure tools are granted.	<p>Observed Access Request Email to determine that the company grants appropriate levels of access to infrastructure tools.</p> <p>Inspected the System Access Control Policy to determine that the Security Officer is required to grant or reject access to systems as dictated by the employee's role and job title and/or as needed.</p>	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel	ProCogia maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inspected the vendor directory which includes a list of vendors along with their categories, risk levels, owners, and links to their Privacy Policy and Terms of Use to determine that the company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	No exceptions noted.



	to meet the entity's objectives.		<p>Inspected High Risk Compliance reports to determine that the company's critical vendor compliance reports are reviewed annually.</p> <p>Inspected the Vendor Management Policy to determine that the company may choose to audit IT vendors and partners to ensure compliance with applicable security policies, as well as legal, regulatory and contractual obligations.</p>	
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.	ProCogia performs annual access control reviews.	<p>Inspected the blocked status of an inactive account to determine that the company performs access control reviews and changes the access levels when required.</p> <p>Inspected an email with the distribution list and list of members attached to determine that the company performs annual access control reviews.</p> <p>Inspected the System Access Control Policy to determine that the company is required to perform annual access control reviews.</p>	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	A termination checklist is used to ensure that system access, including physical access, for terminated employees has been removed within one specified time	<p>Inspected the System Access Control Policy to determine that the HR department, users, and their supervisors are required to notify the Security Officer upon completion and/or termination of access needs and facilitate completion of the termination checklist.</p> <p>Disclosure: No employees were terminated during the observation window.</p>	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected	ProCogia maintains a directory of its key vendors, including its	Inspected the vendor directory which includes a list of vendors along with their categories, risk	No exceptions noted.



	information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	agreements that specify terms, conditions and responsibilities.	levels, owners, and links to their Privacy Policy and Terms of Use to determine that the company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities. Inspected the Vendor Management Policy which details the requirements for maintaining a vendor inventory and vendor contracts that must include confidentiality and privacy commitments, to determine that the company is required to maintain a directory of its key vendors, including its agreements that specify terms, conditions, and responsibilities.	
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.	ProCogia has security policies that have been approved by management and detail how physical security for the company's headquarters is maintained. These policies are accessible to all employees and contractors.	Inspected the Physical Security Policy stating the access requirements and building standards for asset security to determine that Physical Security Policy is in place, accessible to employees through Drata, and has been approved by management.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	ProCogia has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors.	Inspected the Physical Security Policy stating the access requirements and building standards for asset security to determine that Physical Security Policy is in place and is accessible to employees through Drata.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over	A termination checklist is used to ensure that system access, including physical access, for	Inspected the System Access Control Policy to determine that the HR department, users, and	No exceptions noted.



	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.	terminated employees has been removed within one specified time	their supervisors are required to notify the Security Officer upon completion and/or termination of access needs and facilitate completion of the termination checklist. Disclosure: No employees were terminated during the observation window.	
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.	ProCogia has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	Inspected the Data Deletion Policy to determine that the requirements and controls/procedures to manage the deletion of customer data have been described. Inspected the Information Security Policy to determine that procedures for the disposal of sensitive data have been described stating that whiteboards containing restricted and/or sensitive information should be erased and the company requires to destroy, delete, erase, or conceal company data, or otherwise making such files or data unavailable or inaccessible to authorized users.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	ProCogia ensures that all connections to its web application from its users are encrypted.	Inspected the security certificate of the company's website which is valid until July 10, 2023, to determine that the company ensures that all connections to its web application from its users are encrypted. Inspected the Data Protection Policy to determine that the company requires all external data transmission to be encrypted end-to-end using encryption keys.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from	WAF in place to protect ProCogia's application from outside threats.	Observed Firewall Settings to determine that the company has WAF in place to protect applications from outside threats.	No exceptions noted.



	sources outside its system boundaries.			
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	ProCogia uses configurations that ensure only approved networking ports and protocols are implemented, including firewalls.	Observed that the built-in firewall feature of AWS has been used by the company to deny all traffic that is not explicitly allowed.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	Observed that the company uses Intruder for vulnerability scanning. Inspected the Data Protection Policy to determine that the company is required to use an intrusion detection system to monitor system and network administration activities.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for external users, and MFA required for employee users.	Inspected the authentication settings showing a contact number that is used for verification upon signing in to determine that authentication is required before access is granted. Inspected the personnel data to determine that all current employees and contractors have identity MFA enabled and have unique email IDs. Inspected the Password Policy to determine that the company requires strong passwords to be used and MFA to be enabled for all systems that provide the option for it.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	ProCogia requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.	Observed that MFA is enabled on all employees' identity provider accounts. Inspected the Password Policy to determine that the company requires MFA to be enabled for all systems that provide the option for MFA.	No exceptions noted.
CC6.6	The entity implements logical access security	ProCogia automatically logs users out after a predefined inactivity	Inspected the personnel data to determine that all employees have	No exceptions noted.



	measures to protect against threats from sources outside its system boundaries.	interval and/or closure of the internet browser, and requires users to reauthenticate	a screensaver lock enabled on their workstations. Inspected the System Access Control Policy to determine that users are required to make information systems inaccessible by any other individual when unattended using a password-protected screen saver or logging off the system.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	ProCogia ensures that all company-issued computers use a screensaver lock with a timeout of no more than 15 minutes.	Inspected the device compliance data to determine that all employees have screensaver lock enabled on their devices. Inspected the System Access Control Policy to determine that the company requires users to make information systems inaccessible by any other individual by using a password-protected screen saver or logging off the system when left unattended.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	ProCogia maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.	Inspected the architecture diagram, last reviewed on November 9, 2022, showing the service architecture and used applications to determine that the company maintains an accurate and current network diagram. Inspected the Asset Management Policy to determine that a network diagram is available to all appropriate service personnel and is kept current.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	ProCogia has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	Inspected the Password Policy to determine that formal guidelines and requirements regarding password length and complexity have been established by the management.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and	ProCogia uses encryption to protect user authentication and admin sessions of the internal	Inspected the security certificate of the website, valid up to June 10, 2023, to determine that the	No exceptions noted.



	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.	admin tool transmitted over the Internet.	company uses encryption to protect sessions conducted over the Internet. Inspected the Data Protection Policy to determine that the company requires all Internet and intranet connections to be encrypted.	
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.	ProCogia ensures that all connections to its web application from its users are encrypted.	Inspected the security certificate of the company's website which is valid until July 10, 2023, to determine that the company ensures that all connections to its web application from its users are encrypted. Inspected the Data Protection Policy to determine that the company requires all external data transmission to be encrypted end-to-end using encryption keys.	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.	ProCogia ensures that company-issued laptops have encrypted hard-disks.	Inspected the personnel data displaying that all employees have hard disk encryption enabled on their workstations to determine that all company-issued laptops have encrypted hard disks. Inspected the System Access Control Policy to determine that the company requires hard drives to be encrypted.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	ProCogia requires antivirus software to be installed on workstations to protect the network against malware.	Inspected the device compliance data to determine that all employees have anti-virus software installed on their workstations. Inspected the Acceptable Use Policy to determine that anti-malware or equivalent protection and monitoring must be installed and enabled on all endpoint systems.	No exceptions noted.



CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	ProCogia's workstation operating system (OS) security patches are applied automatically.	<p>Observed a list of all relevant workstations to determine that OS security patches are applied automatically.</p> <p>Inspected the Asset Management Policy to determine that the company is required to evaluate and install OS patches periodically, according to their criticality, and during off-peak hours.</p>	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	ProCogia has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.	<p>Inspected the 7-day highlights of activity and behavioral metrics of traffic in Jetpack stats to determine that ProCogia has infrastructure logging configured to monitor web traffic and suspicious activity.</p> <p>Inspected the Data Protection Policy to determine that the company uses Azure Monitor and AWS CloudWatch to monitor the entire cloud service operations, if a system failure or alarm is triggered, key personnel are notified by text, chat, and/or email message to take appropriate corrective action.</p>	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	ProCogia ensures that file integrity monitoring (FIM) software is in place to detect whether operating system and application software files have been tampered with.	<p>Inspected the Data Protection Policy to determine that the company is required to enable file integrity monitoring (FIM) for the security of the production systems.</p> <p>Disclosure: No production systems are currently in place at this time.</p>	No exceptions noted.
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)	ProCogia engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Disclosure: ProCogia does not have a physical network and does not store customer data on its cloud environment.	No exceptions noted.



	susceptibilities to newly discovered vulnerabilities.			
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	Observed that the company uses Intruder for vulnerability scanning. Inspected the Data Protection Policy to determine that the company is required to use an intrusion detection system to monitor system and network administration activities.	No exceptions noted.
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.	ProCogia engages with third-party to conduct vulnerability scans of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the vulnerability scan report displaying zero breaches identifies to determine that the company engages with Intruder to conduct vulnerability scans of the production environment. Inspected the Vulnerability Management Policy to determine that the company is required to conduct vulnerability scans of the internal and external network at least annually or after any significant change to the network.	No exceptions noted.
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.	ProCogia has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.	Inspected the 7-day highlights of activity and behavioral metrics of traffic in Jetpack stats to determine that ProCogia has infrastructure logging configured to monitor web traffic and suspicious activity. Inspected the Data Protection Policy to determine that the company uses Azure Monitor and AWS CloudWatch to monitor the entire cloud service operations, if a system failure or alarm is triggered, key personnel are notified by text, chat, and/or email message to take appropriate corrective action.	No exceptions noted.



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.	ProCogia conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Observed that the company uses Drata to perform continuous monitoring of its information controls.	No exceptions noted.
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.	When ProCogia's application code changes, code reviews and tests are performed by someone other than the person who made the code change.	<p>Inspected the Software Development Life Cycle Policy to determine that the company requires code changes to be reviewed by individuals other than the originating code author.</p> <p>Disclosure: ProCogia has not and currently is not developing any product/software.</p>	No exceptions noted.
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.	ProCogia uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	<p>Observed that the company uses GitHub as a version control system. However, it is used only for testing purposes currently.</p> <p>Inspected the Software Development Policy which states the design system components phase transforms requirements into specifications to guide the work of the development phase to determine that the company uses a version control system to manage source code, documentation, release labeling, and other change management tasks.</p>	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious	ProCogia does not use Root Account on Infrastructure provider	Observed that AWS has the root account disabled by default.	No exceptions noted.



	acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2	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.	ProCogia engages with third-party to conduct vulnerability scans of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the vulnerability scan report displaying zero breaches identifies to determine that the company engages with Intruder to conduct vulnerability scans of the production environment. Inspected the Vulnerability Management Policy to determine that the company is required to conduct vulnerability scans of the internal and external network at least annually or after any significant change to the network.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	ProCogia uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.	Inspected the monitoring alerts in Azure to determine that ProCogia uses logging software that sends alerts to appropriate personnel. Inspected the Data Protection Policy to determine that the company uses Azure Monitor and AWS CloudWatch to monitor the entire cloud service operations, if a system failure or alarm is triggered, key personnel are notified by text, chat, and/or email message to take appropriate corrective action.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives;	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	Observed that the company uses Intruder for vulnerability scanning. Inspected the Data Protection Policy to determine that the company is required to use an intrusion detection system to monitor system and network administration activities.	No exceptions noted.



	anomalies are analyzed to determine whether they represent security events.			
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.	ProCogia is using Drata to monitor the security and compliance of its cloud infrastructure configuration	Observed that the AWS infrastructure is linked to Drata to determine that the company uses Drata to monitor the security and compliance of its cloud infrastructure.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	ProCogia's cloud infrastructure is monitored through an operational audit system that sends alerts to appropriate personnel	<p>Inspected the monitoring alerts in Azure to determine that the company uses Azure monitor as an operational audit system that sends alerts to appropriate personnel.</p> <p>Inspected the Data Protection Policy to determine that the company uses Azure Monitor and AWS CloudWatch to monitor the entire cloud service operations, if a system failure or alarm is triggered, key personnel are notified by text, chat, and/or email message to take appropriate corrective action.</p>	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether	ProCogia tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Observed that security issues are tagged and prioritized in ClickUp.	No exceptions noted.



	they represent security events.			
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.	ProCogia has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.	<p>Inspected the 7-day highlights of activity and behavioral metrics of traffic in Jetpack stats to determine that ProCogia has infrastructure logging configured to monitor web traffic and suspicious activity.</p> <p>Inspected the Data Protection Policy to determine that the company uses Azure Monitor and AWS CloudWatch to monitor the entire cloud service operations, if a system failure or alarm is triggered, key personnel are notified by text, chat, and/or email message to take appropriate corrective action.</p>	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.	ProCogia has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.	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.	The security team communicates important information security events to company management in a timely manner.	<p>Inspected the Incident Response Plan to determine that when an information security incident is identified or detected, users are required to notify their immediate manager within 24 hours and the manager should immediately notify the ISM on call for a proper response.</p> <p>Disclosure: No security incidents occurred during the observation window.</p>	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether	ProCogia has implemented an Incident Response Policy that includes creating, prioritizing,	Inspected the Incident Response Plan to determine that the company has defined the incident	No exceptions noted.



	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.	assigning, and tracking follow-ups to completion.	response process, which requires conducting a post-mortem that includes root cause analysis and documentation of any lessons learned. Disclosure: No security incidents occurred during the observation window.	
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.	ProCogia tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Observed that security issues are tagged and prioritized in ClickUp.	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.	ProCogia has implemented an Incident Response Policy that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team.	Inspected the Incident Response Plan to determine that the company requires the ISM to conduct a post-mortem after an incident has been resolved that includes root cause analysis and documentation of any lessons learned. Disclosure: No security incidents occurred during the observation window.	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.	ProCogia has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents. Disclosure: No security incidents occurred during the observation window.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing	ProCogia has an established Incident Response Policy that outlines management	Inspected the Incident Response Plan to determine that the process of establishing and executing the	No exceptions noted.



	a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.	
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.	ProCogia has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents. Disclosure: No security incidents occurred during the observation window.	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.	ProCogia tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Observed that security issues are tagged and prioritized in ClickUp.	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.	ProCogia has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-ups to completion.	Inspected the Incident Response Plan to determine that the company has defined the incident response process, which requires conducting a post-mortem that includes root cause analysis and documentation of any lessons learned. Disclosure: No security incidents occurred during the observation window.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain,	ProCogia has implemented an Incident Response Policy that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and	Inspected the Incident Response Plan to determine that the company requires the ISM to conduct a post-mortem after an incident has been resolved that includes root cause analysis and	No exceptions noted.



	remediate, and communicate security incidents, as appropriate.	sharing them with the broader engineering team.	documentation of any lessons learned. Disclosure: No security incidents occurred during the observation window.	
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	ProCogia performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	Observed that all AWS clusters are backed up daily to determine that the company performs daily data backups. Inspected the Backup Policy to determine that the company is required to perform automatic backups of its databases on a daily basis.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	ProCogia has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents. Disclosure: No security incidents occurred during the observation window.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	ProCogia has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	ProCogia tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Observed that security issues are tagged and prioritized in ClickUp.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from	ProCogia has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-ups to completion.	Inspected the Incident Response Plan to determine that the company has defined the incident response process, which requires conducting a post-mortem that	No exceptions noted.



	identified security incidents.		includes root cause analysis and documentation of any lessons learned. Disclosure: No security incidents occurred during the observation window.	
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	ProCogia has implemented an Incident Response Policy that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team.	Inspected the Incident Response Plan to determine that the company requires the ISM to conduct a post-mortem after an incident has been resolved that includes root cause analysis and documentation of any lessons learned. Disclosure: No security incidents occurred during the observation window.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	ProCogia ensures that incident response plan testing is performed on an annual basis.	Inspected the tabletop exercises which include test scenarios, discussions, and steps for analyzing and mitigating the issue to determine that the company performs annual testing. Inspected the Incident Response Plan to determine that the company is required to test the plan annually.	No exceptions noted.
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.	Only authorized ProCogia personnel can push or make changes to production code.	Disclosure: The company is not using the version control system and the code repository to build any internal or client product.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data,	ProCogia has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inspected the Software Development Life Cycle Policy which prescribes the phases of the software development life cycle as well as SDLC security control guidelines , to determine that the company has developed policies	No exceptions noted.



	software, and procedures to meet its objectives.		and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	
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.	ProCogia uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	Observed that the company uses GitHub as a version control system. However, it is used only for testing purposes currently. Inspected the Software Development Policy which states the design system components phase transforms requirements into specifications to guide the work of the development phase to determine that the company uses a version control system to manage source code, documentation, release labeling, and other change management tasks.	No exceptions noted.
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.	ProCogia ensures that releases are approved by appropriate members of management prior to production release.	Disclosure: The company is not using the version control system and the code repository to build any internal or client product.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	ProCogia utilizes multiple availability zones to replicate production data across different zones.	Observed Backup Settings to determine that the company utilizes multiple availability zones to replicate production data across different zones. Inspected the Backup Policy to determine that 0965688 BC LTD performs automatic backups of this aforementioned data to protect against catastrophic loss due to unforeseen events that impact the entire system. An automated process will back up all data to Microsoft Azure. This data	No exceptions noted.



			is backed up daily. Backups are monitored and alerted. Backup failures trigger an email notification to the admin of the data pipeline.	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	ProCogia has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-ups to completion.	<p>Inspected the Incident Response Plan to determine that the company has defined the incident response process, which requires conducting a post-mortem that includes root cause analysis and documentation of any lessons learned.</p> <p>Disclosure: No security incidents occurred during the observation window.</p>	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	ProCogia has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	<p>Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.</p> <p>Disclosure: No security incidents occurred during the observation window.</p>	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	ProCogia maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	<p>Inspected the cyber security coverage document issued by Lloyd's Underwriters to determine that the company maintains coverage against cybersecurity risks.</p> <p>Inspected the Risk Assessment Policy to determine that the company may transfer risk to a third party by purchasing an insurance policy.</p>	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	ProCogia performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	<p>Observed that all AWS clusters are backed up daily to determine that the company performs daily data backups.</p> <p>Inspected the Backup Policy to</p>	No exceptions noted.



			determine that the company is required to perform automatic backups of its databases on a daily basis.	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	ProCogia has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	ProCogia has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Disaster Recovery Plan to determine that the disaster recovery procedure and the roles and responsibilities of the Security Officer for the implementation of recovery procedures have been defined by the company.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	ProCogia has implemented an Incident Response Policy that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team.	Inspected the Incident Response Plan to determine that the company requires the ISM to conduct a post-mortem after an incident has been resolved that includes root cause analysis and documentation of any lessons learned. Disclosure: No security incidents occurred during the observation window.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	ProCogia maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inspected the vendor directory which includes a list of vendors along with their categories, risk levels, owners, and links to their Privacy Policy and Terms of Use to determine that the company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities. Inspected High Risk Compliance reports to determine that the company's critical vendor	No exceptions noted.



			<p>compliance reports are reviewed annually.</p> <p>Inspected the Vendor Management Policy to determine that the company may choose to audit IT vendors and partners to ensure compliance with applicable security policies, as well as legal, regulatory and contractual obligations.</p>	
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	ProCogia maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	<p>Inspected the vendor directory which includes a list of vendors along with their categories, risk levels, owners, and links to their Privacy Policy and Terms of Use to determine that the company maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.</p> <p>Inspected the Vendor Management Policy which details the requirements for maintaining a vendor inventory and vendor contracts that must include confidentiality and privacy commitments, to determine that the company is required to maintain a directory of its key vendors, including its agreements that specify terms, conditions, and responsibilities.</p>	No exceptions noted.

