SOC 2 Type 2 Report

Chronicled

November 4, 2022 to August 4, 2023
Next Audit Window: August 5, 2023 to August 4, 2024

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

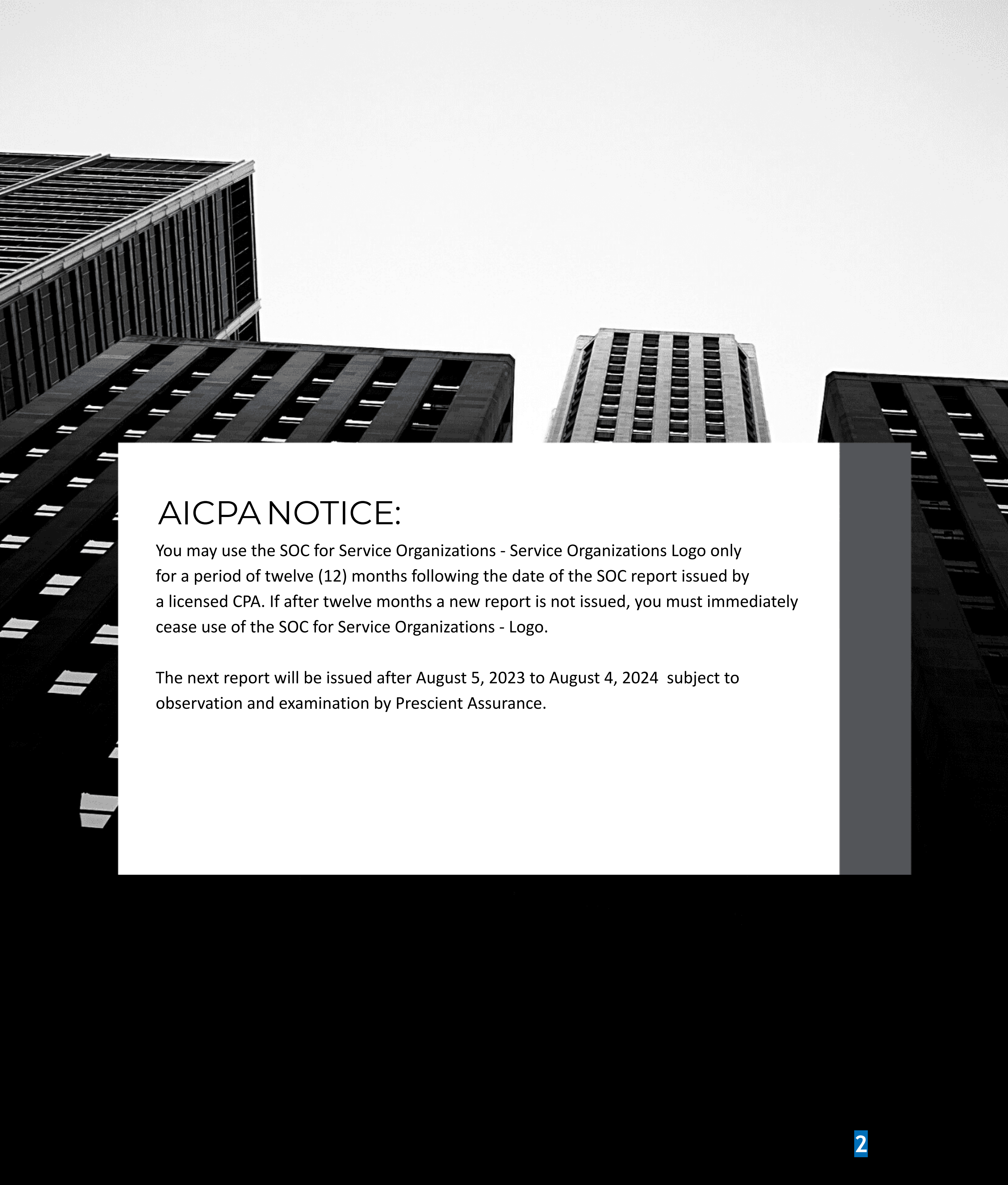
AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

CPA

Prescient Assurance LLC.
1100 Market Street Suite 600
Chattanooga, TN 37402

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319



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 will be issued after August 5, 2023 to August 4, 2024 subject to observation and examination by Prescient Assurance.

Table of Contents

SECTION 1

Management's Assertion

Management's Assertion

We have prepared the accompanying description of Chronicled's system throughout the period November 4, 2022, to August 4, 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 Chronicled's system that may be useful when assessing the risks arising from interactions with Chronicled's system, particularly information about system controls that Chronicled 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*.

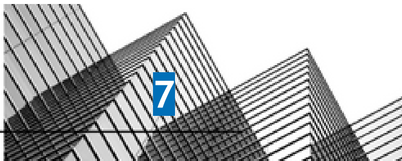
Chronicled uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Chronicled, to achieve Chronicled 's service commitments and system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

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

a. The description presents Chronicled's system that was designed and implemented throughout the period November 4, 2022, to August 4, 2023 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period November 4, 2022, to August 4, 2023, to provide reasonable assurance that Chronicled'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 Chronicled's controls during that period.
c. The controls stated in the description operated effectively throughout the period November 4, 2022, to August 4, 2023, to provide reasonable assurance that Chronicled'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 Chronicled's controls operated effectively throughout the period.

Ravikumar Venkatesan
Director of Engineering - QA
Chronicled



SECTION 2

Independent Service Auditor's Report

Independent Service Auditor's Report

To: Chronicled

Scope

We have examined Chronicled's ("Chronicled") accompanying description of its Chronicled system found in Section 3, titled Chronicled System Description throughout the period November 4, 2022, to August 4, 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 November 4, 2022, to August 4, 2023, to provide reasonable assurance that Chronicled'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*.

Chronicled 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 Chronicled, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents Chronicled's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Chronicled'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 Chronicled, to achieve Chronicled's service commitments and system requirements based on the applicable trust services criteria. The description presents Chronicled's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Chronicled'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

Chronicled 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 Chronicled's service commitments and system requirements were achieved. In Section 1, Chronicled has provided the accompanying assertion titled "Management's Assertion of Chronicled" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Chronicled 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:

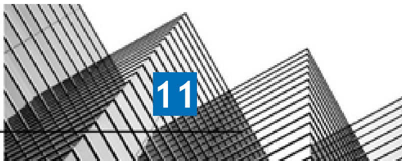
a. The description presents Chronicled's system that was designed and implemented throughout the period November 4, 2022, to August 4, 2023, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period November 4, 2022, to August 4, 2023, to provide reasonable assurance that Chronicled'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 Chronicled's controls throughout the period.
c. The controls stated in the description operated effectively throughout the period November 4, 2022, to August 4, 2023, to provide reasonable assurance that Chronicled'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 Chronicled's controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of Chronicled, user entities of Chronicled's system during some or all of the period November 4, 2022 to August 4, 2023, business partners of Chronicled 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

John D. Wallace, CPA
Chattanooga, TN
November X, 2023

SECTION 3

System Description

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

Chronicled Inc (Chronicled or the Company) was established in 2014 and is located in San Francisco, California. The Company provides services to pharmaceuticals and is the custodian of the Mediledger network, an industry lead, blockchain-powered network within the life sciences industry. These services are provided using the Chronicled Software System which has been built using blockchain technology.

Chronicled is a technology company that provides the following services:

- Automation to share company rosters and contracts with other companies in the Life Sciences industry.
- Enable automation, trust, and automatic settlement for transactions between companies in the Life Sciences industry.
- Provide Network as a Platform with protocol primitives established for any kind of information or transaction shared between companies.

This report describes the internal controls in operations related to the services provided at all Chronicled business locations and is intended to provide reasonable assurance as to the presence of controls relating to the security and availability criteria included in the 2017 AICPA Trust Services Criteria and information to interested parties so that they may better understand our controls as they relate to their use of the Service.

DC 2: The Principal Service Commitments and System Requirements

Chronicled designs its processes and procedures related to the security System to meet its objectives for its services. Those objectives are based on the service commitments that Chronicled makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that Chronicled has established for the services. Security and availability commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Encrypt data at rest
- Encrypt data in transit
- Requiring multiple operators to confirm critical changes

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

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

3.1 Primary Infrastructure

The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services.

Laptops are used by company employees for their development work, connecting to test and production networks, deployment and troubleshooting. Employees also use laptops as a company asset to take Zoom calls and communicate with internal and external (customers) entities.

Virtual environment in Google Cloud Platform (GCP) is used by Chronicled to host the solution in test and production environments.

Jamf account is used to manage the company laptops given to employees to accomplish their work related tasks.

Employees have zoom accounts that they use to communicate with internal and external entities. Slack is used for internal communication between employees.

Prometheus and Grafana are used for monitoring the test and production environment.

3.2 Primary Software

The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.

Postgres database is used by the application internally to save data. The application in use is a desktop application. Customers spin off their own nodes that connect to the cloud node which is used to setup the network.

3.3 People

The personnel involved in the governance, management, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).

Board of Directors is responsible for the following:

- Oversight of the business objectives
- Assure operational management team performs their fiduciary duties
- Evaluate financial burndown
- Look out for company funding
- Measure and evaluate company equity
- Set/Evaluate overall company vision

Management team is responsible for the following:

- Come up with a roadmap for the upcoming releases
- Assure product aligns with business objectives
- Prioritize the deliverables for releases
- Set up processes that are required for the development and deliverables
- Performance management of the team

Devops/Security committee is a cared out virtual team and they are involved in the governance of the test and production environment. We have a small committee of developers who have access to make changes to these customer-facing environments.

Engineers are employees who help to develop the product based on the requirements from customers and product management.

3.4 Data

Databases are used to store customer entered information that is required for the business logic to work.

Configuration files that are required for the proper execution of the system to serve customer requests.

Flat files like csv that are delivered to the customers as an output of the system.

Boundaries of the System

Processes External to Chronicled

- Authority Data Verification: DEA, HIN, and 340B data verification is processed via their respective entities. Chronicled only performs data retrieval and upload Authority Data
- Financial Transactions: Chronicled only provides the data for financials. Actual financial transactions are processed and owned by third-party entities external to Chronicled.
- Model N Contract Management: Contract processing is performed by Model N. Chronicled only consumes the data provided by Model N (owned by participants and customers) and assumes all data is up-to-date and correct.

3.5 Third-party Products and Access

- On-Premise Solution Requirements: Currently, Chronicled products and services can be on-premise. All hardware and software dependencies (e.g., CPU, memory, data storage, operating systems, anti-virus, etc.) for on-premise solutions are managed by the participant (i.e., the customers).

- Chronicled Hosted Solution Requirements: Currently, Chronicled products and services can be hosted. All hardware and software dependencies (e.g., CPU, memory, data storage, operating systems, anti-virus, etc.) for hosted solutions run on third-party managed cloud resources that are configured by Chronicled.
- Model N: Chronicled connects to Model N's database for the purposes of read-only retrieval of processed data (i.e., contracts and customers).
- The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Automated Procedures:

- We have alerts in the prod and test net which posts to Slack and notifies the team about the issues in the setup.
- We have an automated process to deploy once the changes to the production environment are approved by personnel who are responsible for the production and test environment.

Manual Procedures:

- Create tickets as part of VUL scans that we find on weekly basis

Policies are discussed and decided by the security committee. They are rolled out by the security committee once approved.

For any changes to the environment based on the policy that is defined we need approval from a minimum of two people. This includes environment creation and update. Once the changes are approved and merged, the automated deployment process is triggered. Access to the environment is secured via VPN and TLS.

Access to the environment that is required by developers is controlled only to a handful of users. These users can provide the information by pulling in the log files and attaching it to the internal tracking system.

Devops performs system monitoring via automation and manual techniques. Automated monitoring is composed of Prometheus and Grafana. Accessing the environment is via authentication.

System environment implementation and/or change is executed with three distinct protocols: environment creation and update, environment debugging, and monitoring. The three protocols assure the system's adherence to business and security requirements.

Environment Creation and Update

A minimum of two people approve a change or new implementation Environment Debugging

DC 4: Disclosures about Identified Security Incidents

No incidents have occurred to our infrastructure or services since our last review.

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

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

5.1 Management Philosophy

Chronicled's management philosophy directly affects the control environment. The company believes in transparency and integrity—adhering and exceeding industry standards—to assure customer trust.

To execute this vision, Chronicled's Security, Quality, and Compliance Steering Board has established a set of protocols and procedures to capture, evaluate, and remediate any necessary implementations or changes to our compliance policies. The Steering Board is represented by individuals from the company's established departments of Development, Devops, Quality Assurance, and Professional Services.

All implementations and changes to Chronicled's compliance protocols are always reviewed and evaluated with these overarching philosophies and goals:

- meeting or exceeding standards,
- establishing and retaining customer satisfaction and trust,
- and the continuing of transparency across all stakeholders.

5.2 Security Policies

The following security policies and related processes are in place for the Chronicled System:

- We adhere to Multifactor authentication (MFA) for Chronicled's used services.
- Manage user access
- Manage changes to the environment using a process that is controlled by a limited set of engineers
- Use Terraform in the environment so that it can be well managed and configured consistently

Any changes to the environment are managed within a controlled way. Every change is tracked using a Jira ticket that is assigned to an individual. Engineers can put out a review to make changes but are only approved by a few engineers who are part of the committee to manage the environment.

5.3 Personnel Security

All hires are supported by job descriptions. Before hiring, background checks are performed for new hires. Employees are hired contingent upon background checks. Once employees are hired they have to go through security, anti-phishing, and privacy and data protection training.

5.4 Physical Security and Environmental Controls

Chronicled's environment is all virtual. We have our systems hosted from Google Cloud Services Platform (GCP). We have our controls in place to make any change to the environment. Access to the environment is governed by access control given to a handful of experts to monitor and maintain the systems.

5.5 Change Management

Chronicled has a formalized change management process in place. Proposed changes are reviewed by engineers and only approved by a committee that manages the environment. Any changes that get into production are tested internally. All changes are tracked using the change management system (Jira).

Emergency changes follow the formalized change management process but at an accelerated timeline. Prior to initiating an emergency change, necessary approvals are obtained and documented.
Changes to infrastructure and software are developed and tested in a separate development and/or test environment before implementation. Additionally, all developers do not have the ability to migrate changes into production environments.

5.6 System Monitoring

The security administration team uses a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, intrusion detection system (IDS) alerts, and vulnerability notifications. These alerts and notifications are reviewed weekly by the security administration team. Additionally, the security administration team has developed and will review the following reports:

- IDS attacks
- Firewall configuration changes
- Security events requiring further investigation are tracked using tickets

Problem Management

Security incidents and other IT-related problems are reported over slack and ticketing system.

5.7 Data Backup and Recovery

Chronicled uses data backup software to backup data in the cloud. Access to backups, scheduling utilities, systems is restricted to authorized personnel.

5.8 System Account Management

Chronicled has strict control over access to the production environment. Employees are granted access only upon approval. User access is verified on hiring and termination.
The human resources department provides DevOps personnel with an employee termination checklist whenever there are departures. DevOps reconciles the termination checklist with current access privileges to determine if access has been appropriately removed.

5.9 Risk Assessment Process

Chronicled regularly reviews the risks that may threaten the achievement of its service commitments and system requirements.

DevOps team opens tickets in the ticketing system for any vulnerabilities that are found on an ongoing basis.

Changes in security threats and risks are reviewed by Chronicled, and updates to existing control activities and information security policies are performed as necessary.

5.10 Information and Communication Systems

Chronicled has an information security policy to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of appropriate realtime channels to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems.

5.11 Monitoring Controls

Chronicled DevOps team uses vulnerability alerts we get from quay.io and opens tickets in a ticketing system to track them.

DC 6: Complementary User Entity Controls (CUECs)

Chronicled, Inc. services and controls were designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at user organizations is necessary to achieve certain control objectives included in this report.

There may be additional controls in operation at user organizations to complement the control objectives identified in this report. In addition to those user control considerations, auditors of user organizations should consider whether the following controls have been placed in operation at user organizations.

Controls Associated	User Entity Control Considerations
Testnet, Devnet, and Prodnet access	Users are responsible to make changes and publish them to their respective hosted environment. These users are also able to monitor their environment if needed to help debug issues.
Whitelisting customers	Customers are responsible for opening their firewall ports in order for the product to work correctly with the partners they wish to do business with.

The list of user entity control considerations presented above do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations.

DC 7: Complementary Subservice Organization Controls (CSOCs)

Chronicled, Inc. controls related to the System cover only a portion of overall internal control for each user entity of Chronicled, Inc. It is not feasible for the control objectives related to services to be achieved solely by Chronicled, Inc. Therefore, each user entity's internal control over Chronicled, Inc. system must be evaluated in conjunction with the security controls and system requirements represented in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Controls Associated	Subservice Organization Control
Google Cloud Platform (GCP)	Only selected members of the team are allowed to make changes to the test and production environments. Apart from that all other members of the engineering team are allowed to deploy in functional and dev clusters in GCP.

The list of complementary subservice organization controls presented herein does not represent a comprehensive set of all the controls performed by the subservice organization. The list above notes controls that must be operating effectively within the subservice organization to provide reasonable assurance that the Chronicled, Inc. controls stated within Section 4 of this report are able to operate effectively.

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

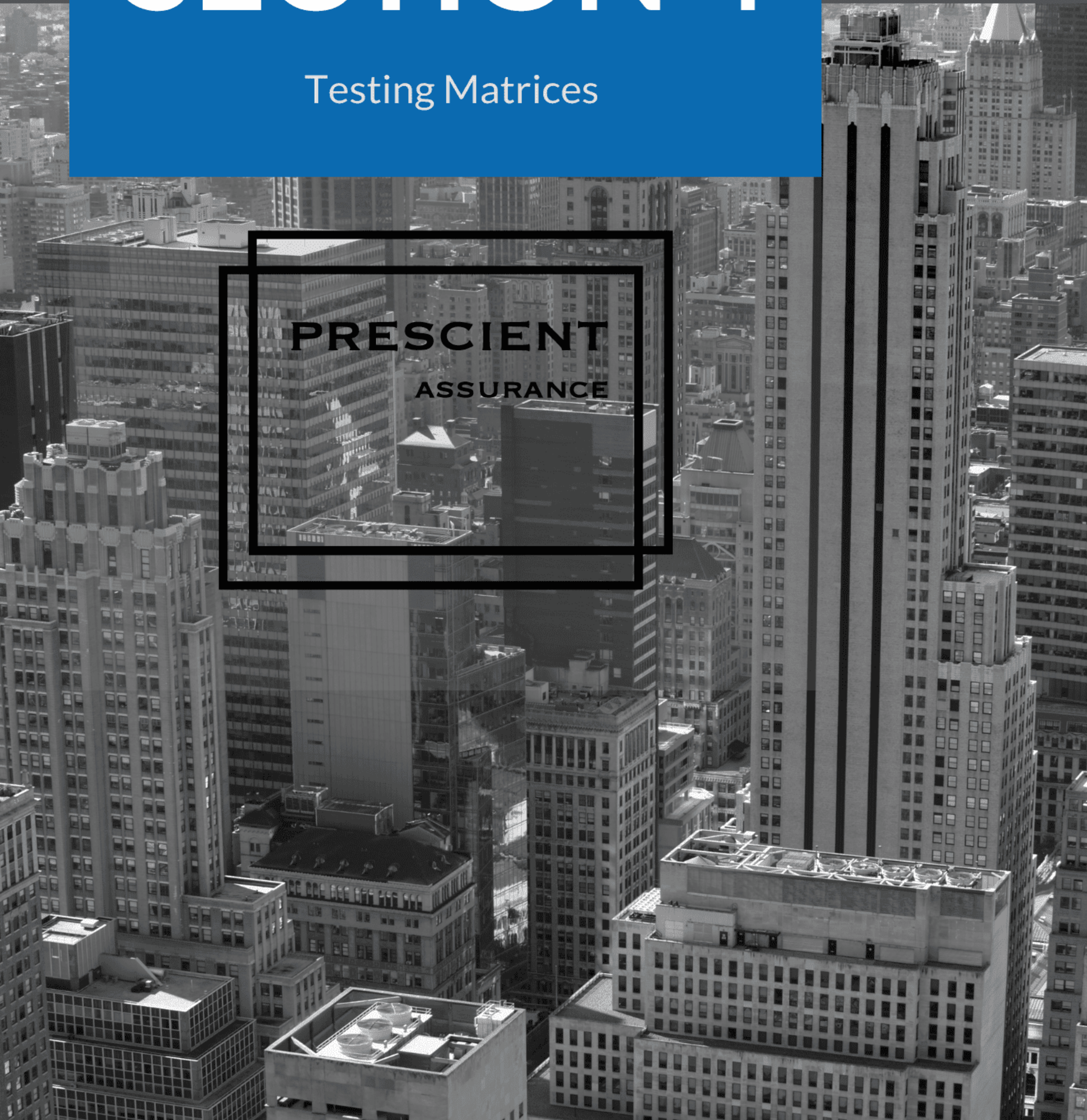
All Security criteria were applicable to the system in scope.

DC 9: Disclosures Of Significant Changes In Last 1 Year

No significant changes have occurred to our infrastructure or services since our last review.

SECTION 4

Testing Matrices



PRESCIENT ASSURANCE

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to Chronicled provided by Chronicled. The scope of the testing was restricted to Chronicled, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing throughout the period November 4, 2022 to August 4, 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: ● 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 ● 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**
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	COSO Principle	Control Description	Test Applied by the Service Auditor	Test Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company performs background checks on new employees.	Observed that the company uses Checkr as a vendor for background checks. Inspected background check records for three sampled personnel to determine that new employees are required have completed their background checks.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected a signed consulting agreement to determine that contractors are required to sign an agreement at the time of engagement acknowledging their commitment to act in compliance with applicable laws.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the Employee Code of Conduct to determine that the company requires all employees to follow the policy. Observed that the Employee Code of Conduct also defines the disciplinary actions against employees who repeatedly or intentionally fail to follow the policies. Inspected the policy acceptance data to determine that all employees have acknowledged the Employee Code of Conduct.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected a signed consulting agreement, which states the nondisclosure and confidentiality terms to determine that contractors are required to sign a confidentiality agreement at the time of engagement.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to sign a confidentiality agreement during onboarding.	Observed two samples of signed proprietary information and inventions agreements to determine that the company requires its employees to sign a confidentiality agreement at the time of engagement.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company managers are required to complete performance evaluations for direct reports at least annually.	Observed reports of performance evaluations to determine that Chronicled managers are required to complete performance evaluations for direct reports at least annually.	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 regular meeting of the BoD, held on November 30, 2022, to determine that the board of directors meets at least annually to discuss strategy and product updates and other internal matters. Observed that the company's BoD includes independent members to determine that the company requires the board to have independent directors.	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 bios of the Board of Directors to determine that the board members have adequate expertise to lead the management team and oversee the company's internal controls.	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 regular meeting of the BoD, held on November 30, 2022, to determine that the board of directors meets at least annually to receive briefings regarding strategy and product updates and other internal matters.	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 has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the Bylaws of the company to determine that the responsibilities of the Board of Directors to lead internal matters have been defined.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the Bylaws of the company to determine that the responsibilities of the Board of Directors to lead internal matters have been defined.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Security Policy to determine that the Information Security Officer and Information Security Committee are responsible for the development and implementation of information security programs and controls.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Observed an Organizational Chart to determine that the company maintains an organizational chart that describes the organizational structure and reporting lines.	No exceptions noted.

CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Security Policy to determine that the Information Security Officer and Information Security Committee are responsible for the development and implementation of information security programs and controls.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Observed reports of performance evaluations to determine that Chronicled managers are required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company performs background checks on new employees.	Observed that the company uses Checkr as a vendor for background checks. Inspected background check records for three sampled personnel to determine that new employees are required have completed their background checks.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Security Policy to determine that the Information Security Officer and Information Security Committee are responsible for the development and implementation of information security programs and controls.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected the security awareness training data to determine that all relevant employees have completed the mandatory security awareness training.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the Employee Code of Conduct to determine that the company requires all employees to follow the policy. Observed that the Employee Code of Conduct also defines the disciplinary actions against employees who repeatedly or intentionally fail to follow the policies. Inspected the policy acceptance data to	No exceptions noted.

			determine that all employees have acknowledged the Employee Code of Conduct.	
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Security Policy to determine that the Information Security Officer and Information Security Committee are responsible for the development and implementation of information security programs and controls.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Observed reports of performance evaluations to determine that Chronicled managers are required to complete performance evaluations for direct reports 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.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the cloud infrastructure data that GitHub, G Suite Admin, Jira, Confluence, CustomerCheckr, GCP, and Slack infrastructures are linked to Vanta to determine that activities on these applications are tracked on Vanta. Inspected the GCP resources data that all GCP subnets have VPC flow logs enabled, all GCP log sinks, storage buckets, pub/sub-topics, and BigQuery datasets are known to Vanta, logs are centrally stored in GCP, and retained for 365 days, and only authorized users can access tracked GCP log sinks to only authorized users to determine that log management is utilized.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Risk Management Plan to determine that the company is required to perform internal and external vulnerability scans that are performed quarterly and annually. Observed the list of identified vulnerabilities to determine that the company uses GitHub, which is configured on Vanta, to perform host-based vulnerability scans on all external-facing systems. Observed the history of remediated vulnerabilities to determine that critical and high vulnerabilities are tracked to remediation. Inspected the tracking data to determine that the records of security issues are tracked on GitHub.	No exceptions noted.

CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the Risk Management Plan to determine that the company is required to perform a formal risk assessment on an annual basis. Observed that the company uses Vanta for continuous security monitoring.	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 company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected the security awareness training data to determine that all relevant employees have completed the mandatory security awareness training.	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 company communicates system changes to authorized int ernal users.	Observed the release notifications to determine that the company uses Slack to communicate the system modifications to authorized internal users.	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.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Security Policy to determine that the Information Security Officer and Information Security Committee are responsible for the development and implementation of information security programs and 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.	The company provides a description of its products and services to internal and external users.	Observed the network diagram showing the GCP environments signifying the relationships and flows between ports to determine that the company provides the workflow of its services to internal users. Observed the resource section on the company's website to determine that a description of the company's services and solutions is provided online to external users.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and	The company management has established defined roles and responsibilities to	Inspected the Security Policy to determine that the Information Security Officer and Information Security Committee are responsible for the development and	No exceptions noted.

	responsibilities for internal control, necessary to support the functioning of internal control.	oversee the design and implementation of information security controls.	implementation of information security programs and controls.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the information security policies to determine that the company has established security policies and reviews them annually.	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 company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Information Security Incident Response to determine that the incident response procedure and roles and responsibilities of response team members to report, resolve, and document security and privacy incidents have been documented. Inspected the policy acceptance data to determine that all employees have acknowledged the Information Security Incident Response.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Observed the network diagram showing the GCP environments signifying the relationships and flows between ports to determine that the company provides the workflow of its services to internal users. Observed the resource section on the company's website to determine that a description of the company's services and solutions is provided online to external users.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the release notes of the company, which includes release summary, fixes and major issues, to determine that the company provides guidelines and technical support resources relating to system operations to customers. Inspected the FAQ page on the company's website which shows answers to different questions for various topics to determine that the company provides necessary guidelines and technical support resources to customers.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has an external-facing support system in place that allows users to report system information on failures, incidents,	Inspected the community topics page on the company's website which has a general discussion thread and an option to submit a request to determine that an external-facing support system is in place.	No exceptions noted.

		concerns, and other complaints to appropriate personnel.		
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the Third-Party Management Policy to determine that the company requires agreements to be signed with vendors to acknowledge their confidentiality, integrity, availability, and privacy commitments. Observed the vendor inventory to determine that the company has maintained a list of vendors along with their risk levels. Inspected the GCP Terms of service to determine that the confidentiality and privacy commitments of the vendors are documented. Inspected the company's Privacy Policy to determine that privacy, security, and service commitments have been communicated to vendors through the publicly available website.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company notifies customers of critical system changes that may affect their processing.	Inspected the release notes of the company which includes release summary, fixes and major issues to determine that the company notifies customers of critical system changes that may affect their processing. Inspected the Grafana monitoring dashboard which monitors the production nodes to determine that the company notifies customers of critical system changes that may affect their processing.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected a template of an order form which states customer details and additional terms to determine that service and privacy commitments are communicated to customers through official documents. Inspected the Privacy Policy on the company's website to determine that security commitments are communicated to customers through the official website.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the Risk Management Policy to determine that the risk management processes along with design and implementation of risk management controls have been documented that help the company achieve its business objectives. Inspected a snapshot of the risk register, dated July 31, 2023, which shows risk scenarios, scores, and treatment plans to determine that the company is required to identify and mitigate risks that hinder the achievement of its business objectives.	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.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	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.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery Plan to determine that a disaster recovery test is required to be performed on an annual basis. Inspected the policy acceptance data to determine that all employees have agreed to the Business Continuity and Disaster Recovery Plan. Inspected the details of the recovery test scenario which was performed on July 19, 2023, to determine that the company tests the BC/DR at least annually.	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.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed.	Inspected the Risk Management Policy to determine that the company is required to perform a formal risk assessment at least annually. Inspected a snapshot of the risk register, dated July 31, 2023, which shows risk scenarios, scores, and treatment plans to determine that the company is required to identify and mitigate risks that hinder the achievement of its business objectives.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks	The company has a vendor management program in place. Components of this	Inspected the Third Party Management Policy to determine that the third-party risk management, security standards, and vendors' service review and monitoring requirements	No exceptions noted.

	as a basis for determining how the risks should be managed.	program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	have been described. Observed the vendor inventory to determine that the company has maintained a list of vendors along with their risk levels. Inspected the vendor directory to determine that the company has a compliance security report for Google Workspace; all other vendors are low/medium risk.	
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed.	Inspected the Risk Management Policy to determine that the company is required to perform a formal risk assessment at least annually. Inspected a snapshot of the risk register, dated July 31, 2023, which shows risk scenarios, scores, and treatment plans to determine that the company is required to identify and mitigate risks that hinder the achievement of its business objectives.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the Penetration Test report provided by IOActive on November 2, 2022 to determine that a penetration test is performed at least annually, but is not due to be performed during the observation window.	No performance.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed.	Inspected the Risk Management Policy to determine that the company is required to perform a formal risk assessment at least annually. Inspected a snapshot of the risk register, dated July 31, 2023, which shows risk scenarios, scores, and treatment plans to determine that the company is required to identify and mitigate risks that hinder the achievement of its business objectives.	No exceptions noted.

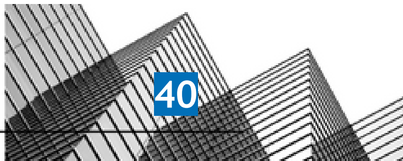
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the company's Core Engineering Processes to determine that the company has established a change management process including the steps of testing, reviewing, obtaining approvals, and developing software.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	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.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the Third Party Management Policy to determine that the third-party risk management, security standards, and vendors' service review and monitoring requirements have been described. Observed the vendor inventory to determine that the company has maintained a list of vendors along with their risk levels. Inspected the vendor directory to determine that the company has a compliance security report for Google Workspace; all other vendors are low/medium risk.	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.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the Penetration Test report provided by IOActive on November 2, 2022 to determine that a penetration test is performed at least annually, but is not due to be performed during the observation window.	No performance.
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.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the Risk Management Plan to determine that the company is required to perform a formal risk assessment on an annual basis. Observed that the company uses Vanta for continuous security monitoring.	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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Risk Management Plan to determine that the company is required to perform internal and external vulnerability scans that are performed quarterly and annually. Observed the list of identified vulnerabilities to determine that the company uses GitHub, which is configured on Vanta, to perform host-based vulnerability scans on all external-facing systems. Observed the history of remediated vulnerabilities to determine that critical and high vulnerabilities are tracked to remediation. Inspected the tracking data to determine that the records of security issues are tracked on GitHub.	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.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the Third Party Management Policy to determine that the third-party risk management, security standards, and vendors' service review and monitoring requirements have been described. Observed the vendor inventory to determine that the company has maintained a list of vendors along with their risk levels. Inspected the vendor directory to determine that the company has a compliance security report for Google Workspace; all other vendors are low/medium risk.	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.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the Risk Management Plan to determine that the company is required to perform a formal risk assessment on an annual basis. Observed that the company uses Vanta for continuous security monitoring.	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.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the information security policies to determine that the company has established security policies and reviews them annually.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks	The company has a documented risk management program in place that includes	Inspected the Risk Management Policy to determine that the company has a documented risk management program in place that includes guidance on the identification of	No exceptions noted.

	to the achievement of objectives to acceptable levels.	guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the information security policies to determine that the company has established security policies and reviews them annually.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Third Party Management Policy to determine that the company requires third parties to maintain a secure development program consistent with industry software and systems development best practices including risk assessment, formal change management, code standards, code review, and testing. Inspected the company's Core Engineering Processes to determine that the company has established a change management process including the steps of testing, reviewing, and developing software.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Security Policy to determine that access approvals are required to be accomplished using Jira tickets and explicit approvals from personnel. Observed Jira tickets for access creations and modifications to determine that the company uses Jira to track access modifications.	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.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the System and Security Monitoring Policy to determine that the company requires system and events logs to be retained. Observed data management system configuration to determine that Chronicled has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. Observed the monthly backup log to determine that the company has retention procedures in place.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish	The company's data backup policy documents requirements for backup	Inspected the Asset Management Policy to determine that the company requires cloud service providers' backups to be used, source	No exceptions noted.

	what is expected and in procedures that put policies into action.	and recovery of customer data.	code in GitHub to be backed up to another service provider daily, and production data in AWS to be backed up to another server in AWS daily.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the company's Core Engineering Processes to determine that the company has established a change management process including the steps of testing, reviewing, obtaining approvals, and developing software. Observed that all relevant GitHub repositories are set to private. Observed code review process to determine that Chronicled requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	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.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Third Party Management Policy to determine that the company requires third parties to maintain a secure development program consistent with industry software and systems development best practices including risk assessment, formal change management, code standards, code review, and testing. Inspected the company's Core Engineering Processes to determine that the company has established a change management process including the steps of testing, reviewing, and developing software.	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.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the information security policies to determine that the company has established security policies and reviews them annually.	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.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Security Policy to determine that the Information Security Officer and Information Security Committee are responsible for the development and implementation of information security programs and controls.	No exceptions noted.
CC5.3	The entity deploys control activities through	The company has a vendor management	Inspected the Third Party Management Policy to determine that the third-party risk	No exceptions noted.

	policies that establish what is expected and in procedures that put policies into action.	program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	management, security standards, and vendors' service review and monitoring requirements have been described. Observed the vendor inventory to determine that the company has maintained a list of vendors along with their risk levels. Inspected the vendor directory to determine that the company has a compliance security report for Google Workspace; all other vendors are low/medium risk.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Information Security Incident Response to determine that the incident response procedure and roles and responsibilities of response team members to report, resolve, and document security and privacy incidents have been documented. Inspected the policy acceptance data to determine that all employees have acknowledged the Information Security Incident Response.	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.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the Risk Management Policy to determine that the risk management processes along with design and implementation of risk management controls have been documented that help the company achieve its business objectives. Inspected a snapshot of the risk register, dated July 31, 2023, which shows risk scenarios, scores, and treatment plans to determine that the company is required to identify and mitigate risks that hinder the achievement of its business objectives.	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.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them	The company requires authentication to production datastores to use authorized secure authentication	Inspected the Asset Management Policy to determine that the company requires each workforce member to be assigned a computer for which they are an administrator and each workforce member’s supervisor to create their unique cloud account.	No exceptions noted.



	from security events to meet the entity's objectives.	mechanisms, such as unique SSH key.	Observed that employees are assigned unique GitHub accounts, all assigned SSH keys are unique, all Google Workspace accounts have MFA enabled, GCP IAM policy bindings do not contain universal role grants, and no GCP role grants assign a critical role to any GCP service account to determine that secure authentication is required before accessing the production datastores.	
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.	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the Cryptography Policy to determine that access to keys and secrets is required to be tightly controlled in accordance with the Access Control Policy. Observed access control permissions to determine that Chronicled restricts privileged access to encryption keys to authorized users with a business need.	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.	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the Data Governance and Management Policy to determine that the company requires all customer nodes containing their data to be provisioned in GCP, and the environments to be guarded with VPN access, firewall rules, and DevOps approvals. Observed that only authorized employees are assigned unique SSH keys to determine that access to firewalls is restricted to authorized personnel with a business need and SSH keys. Observed that all GCP Compute Instances are associated with a GCP network to determine that firewalls are utilized by the company.	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.	The company restricts privileged access to the operating system to authorized users with a business need.	Inspected the Security Policy to determine that there are limited individuals who have access to testnet and prodnet on a permanent basis and access approvals are required to be done using Jira tickets and explicit approval from specific personnel. Observed that service accounts are used in GCP by default. Inspected the accounts' data to determine that employees have unique GitHub accounts. Inspected the GCP resources showing that IAM policy bindings do not contain GCP role grants and GCP role grants do not assign a critical role to any GCP service account to determine that privileged access to the operating system is restricted to authorized users with a business need.	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.	The company restricts privileged access to the production network to authorized users with a business need.	Inspected the Security Policy to determine that there are limited individuals who have access to testnet and prodnet on a permanent basis and access approvals are required to be done using Jira tickets and explicit approval from specific personnel. Observed that service accounts are used in GCP by default. Inspected the accounts' data to determine that employees have unique GitHub accounts. Inspected the GCP resources showing that IAM policy bindings do not contain GCP role grants and GCP role grants do not assign a critical role to any GCP service account to determine that privileged access to the production network is restricted to authorized users with a business need.	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.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the Security Policy to determine that there are limited individuals who have access to testnet and prodnet on a permanent basis and access approvals are required to be done using Jira tickets and explicit approval from specific personnel. Observed access configuration to determine that Chronicled ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	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.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Security Policy to determine that access approvals are required to be accomplished using Jira tickets and explicit approvals from personnel. Observed Jira tickets for access creations and modifications to determine that the company uses Jira to track access modifications.	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.	The company's network is segmented to prevent unauthorized access to customer data.	Inspected a network diagram to determine that Chronicled's network is segmented to prevent unauthorized access to customer data.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure,	The company requires authentication to systems and applications	Inspected the employee account data to determine that all employees have unique version control accounts and all assigned SSH	No exceptions noted.

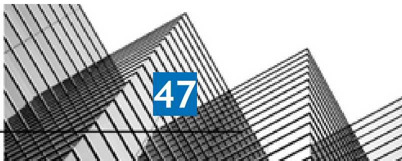
	and architectures over protected information assets to protect them from security events to meet the entity's objectives.	to use unique username and password or authorized Secure Socket Shell (SSH) keys.	keys are special to determine that unique accounts, passwords, and SSH keys are required to access systems and applications.	
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.	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the Asset Management Policy to determine that the password requirements have been documented, which include password length, complexity, and authentication. Observed password configurations to determine that Chronicled requires passwords for in-scope system components to be configured according to the company's policy.	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.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the MFA application data showing that MFA is enabled on all relevant G Suite Admin accounts to determine that the production systems can only be remotely accessed by authorized employees possessing a valid MFA method.	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.	The company's datastores housing sensitive customer data are encrypted at rest.	Observed that user data in Google Cloud Storage is encrypted at rest by default.	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.	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the Data Governance and Management Policy to determine that no one at the company is allowed to get their hands on any customer data without proper approval.	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.	The company restricts access to migrate changes to production to authorized personnel.	Inspected the version control system data showing that the company uses GitHub as a version control system and the visibility of all relevant GitHub repositories has been set to private to determine that the company restricts access to migrate changes to production to authorized personnel.	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.	The company maintains a formal inventory of production system assets.	Inspected the Asset Management Policy to determine that the IT department is required to maintain a software inventory that includes applications developed or used. Inspected the asset inventory which includes GCP resources, GitHub repositories, and computers along with descriptions and assigned owners to determine that the company maintains an inventory of its production system assets and resources.	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.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Observed that SSL/TLS is configured on the admin page of the GCP console. Inspected the devices' data to determine that all employee workstations with the Vanta Agent installed have unique SSH 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 meet the entity's objectives.	The company restricts privileged access to the application to authorized users with a business need.	Observed that employees are assigned unique GitHub accounts, all assigned SSH keys are unique, all Google Workspace accounts have MFA enabled, GCP IAM policy bindings do not contain universal role grants, and no GCP role grants assign a critical role to any GCP service account to determine that access to the application is allowed to users based on business need.	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.	The company restricts privileged access to databases to authorized users with a business need.	Observed that employees are assigned unique GitHub accounts, all assigned SSH keys are unique, all Google Workspace accounts have MFA enabled, GCP IAM policy bindings do not contain universal role grants, and no GCP role grants assign a critical role to any GCP service account to determine that access to the database is allowed to users based on business need.	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.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the security certificate of the website, which is valid until October 14, 2023, to determine that the website is secured using an encrypted connection. Observed that SSL/TLS is enabled on the admin page of the AWS console. Observed access control configuration to determine that Chronicled production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting	The company conducts access reviews at least	Observed a screenshot showing deactivated accounts to determine that the company	No exceptions noted.

	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.	quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	conducts access reviews to help ensure that access is restricted appropriately. Required changes are tracked to completion. Observed that cloud infrastructure and Identity provider are linked to Vanta. Observed three access reviews to determine that Chronicled conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	
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.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Security Policy to determine that access approvals are required to be accomplished using Jira tickets and explicit approvals from personnel. Observed Jira tickets for access creations and modifications to determine that the company uses Jira to track access modifications.	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.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Observed 11 separate employee termination checklists to determine that the company uses a checklist to revoke access of terminated employees and that all employees who were terminated during the observation window had their access revoked within SLA.	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	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Observed that SSL/TLS is configured on the admin page of the GCP console. Inspected the devices' data to determine that all employee workstations with the Vanta Agent installed have unique SSH keys.	No exceptions noted.

	when user access is no longer authorized.			
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.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the Security Policy to determine that there are limited individuals who have access to testnet and prodnet on a permanent basis and access approvals are required to be done using Jira tickets and explicit approval from specific personnel. Observed access configuration to determine that Chronicled ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	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.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Observed that SSL/TLS is configured on the admin page of the GCP console. Inspected the devices' data to determine that all employee workstations with the Vanta Agent installed have unique SSH keys.	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.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Observed 11 separate employee termination checklists to determine that the company uses a checklist to revoke access of terminated employees and that all employees who were terminated during the observation window had their access revoked within SLA.	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	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Observed a screenshot showing deactivated accounts to determine that the company conducts access reviews to help ensure that access is restricted appropriately. Required changes are tracked to completion. Observed that cloud infrastructure and Identity provider are linked to Vanta. Observed three access reviews to determine	No exceptions noted.

	concepts of least privilege and segregation of duties, to meet the entity's objectives.		that Chronicled conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	
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.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the Security Policy to determine that there are limited individuals who have access to testnet and prodnet on a permanent basis and access approvals are required to be done using Jira tickets and explicit approval from specific personnel. Observed access configuration to determine that Chronicled ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	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.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Security Policy to determine that access approvals are required to be accomplished using Jira tickets and explicit approvals from personnel. Observed Jira tickets for access creations and modifications to determine that the company uses Jira to track access modifications.	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.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Observed a screenshot showing deactivated accounts to determine that the company conducts access reviews to help ensure that access is restricted appropriately. Required changes are tracked to completion. Observed that cloud infrastructure and Identity provider are linked to Vanta. Observed three access reviews to determine that Chronicled conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Observed 11 separate employee termination checklists to determine that the company uses a checklist to revoke access of terminated employees and that all employees who were terminated during the observation window had	No exceptions noted.



	those assets has been diminished and is no longer required to meet the entity's objectives.		their access revoked within SLA.	
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.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the System and Security Monitoring Policy to determine that the company requires system and events logs to be retained. Observed data management system configuration to determine that Chronicled has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. Observed the monthly backup log to determine that the company has retention procedures in place.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Inspected the disposal of unused data volumes from the cloud to determine that the company has electronic media containing confidential information purged or destroyed in accordance with best practices	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected the Data Governance and Management Policy to determine that in certain circumstances customer data can be deleted from the database. This can be but is not limited to customer offboarding, and customer requests to clean up a database for any testing performed. Inspected the screenshot of wipe data from AZ Node to determine that the company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the security certificate of the website, which is valid until October 14, 2023, to determine that the website is secured using an encrypted connection. Observed that SSL/TLS is enabled on the admin page of the AWS console. Observed access control configuration to determine that Chronicled production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.

CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Observed that SSL/TLS is configured on the admin page of the GCP console. Inspected the devices' data to determine that all employee workstations with the Vanta Agent installed have unique SSH keys.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the computer inventory to determine that employee computers are monitored with the Vanta agent. Inspected the report of account block warning dated July 10, 2023, to determine that the company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches. Observed that GCP Cloud IDS is enabled on all networks and all projects have notifications configured for GCP Cloud IDS threat detections.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspected the system export data to determine that all GCP Compute Instances are associated with a GCP network. Observed the company's GCP firewall rules to determine that firewalls are configured to prevent unauthorized access. Observed the ingress port review via GitHub to determine that the company reviews its firewall rulesets at least annually.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses firewalls and configures them to prevent unauthorized access.	Inspected the system export data to determine that all GCP Compute Instances are associated with a GCP network. Observed the company's GCP firewall rules to determine that firewalls are configured to prevent unauthorized access.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the record of security issues to determine that security issues are labelled, tracked, prioritized, and assigned owners in GitHub and Jira, and all tasks in GitHub and Jira labelled with security, p1, and p2 tags are marked as complete.	No exceptions noted.
CC6.6	The entity implements logical access security	The company's network and system hardening	Inspected the system export data to determine that all GCP Compute Instances are associated	No exceptions noted.

	measures to protect against threats from sources outside its system boundaries.	standards are documented, based on industry best practices, and reviewed at least annually.	with a GCP network. Observed the company's GCP firewall rules to determine that firewalls are configured to prevent unauthorized access. Observed the ingress port review via GitHub to determine that the company reviews its firewall rulesets at least annually. Observed the list of users with encryption key access to determine that the company restricts encryption key access to authorized users. Observed an access approval ticket to determine that the company has procedures in place to ensure that access is granted based on role.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the Cryptography Policy to determine that sensitive data transmission over the public internet must use TLS protocol. Inspected the security certificate of the website which is valid until October 14, 2023, to determine that the company's website has an unexpired and valid certificate that only accepts TLS connections using up-to-date cipher suites, and redirects HTTP to HTTPS via a 3XX status code.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the MFA application data showing that MFA is enabled on all relevant G Suite Admin accounts to determine that the production systems can only be remotely accessed by authorized employees possessing a valid MFA method.	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.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the Cryptography Policy to determine that sensitive data transmission over the public internet must use TLS protocol. Inspected the security certificate of the website which is valid until October 14, 2023, to determine that the company's website has an unexpired and valid certificate that only accepts TLS connections using up-to-date cipher suites, and redirects HTTP to HTTPS via a 3XX status code.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and	The company has a mobile device management (MDM) system in place to centrally manage mobile	Inspected the data to determine that all employee Windows workstations with the Vanta Agent installed have antivirus software installed.	No exceptions noted.

	protects it during transmission, movement, or removal to meet the entity's objectives.	devices supporting the service.	Observed that the company uses Vanta as an MDM solution.	
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.	The company encrypts portable and removable media devices when used.	Inspected the computer inventory to determine that all employee workstations with the Vanta Agent installed have encrypted hard drives.	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.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Third Party Management Policy to determine that the company requires third parties to maintain a secure development program consistent with industry software and systems development best practices including risk assessment, formal change management, code standards, code review, and testing. Inspected the company's Core Engineering Processes to determine that the company has established a change management process including the steps of testing, reviewing, and developing software.	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.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the record of security issues to determine that security issues are labelled, tracked, prioritized, and assigned owners in GitHub and Jira, and all tasks in GitHub and Jira labelled with security, p1, and p2 tags are marked as complete.	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.	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Inspected the data of the employee workstations to determine that all employee workstations with the Vanta Agent installed have antivirus software installed. Inspected the data to determine that all employee Windows workstations with the Vanta Agent installed have antivirus software installed.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations	The company has a configuration management procedure in place to ensure that system configurations	Inspected the company's Core Engineering Processes to determine that the company has established a change management process including the steps of testing, reviewing, obtaining approvals, and developing software.	No exceptions noted.

	that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	are deployed consistently throughout the environment.		
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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Risk Management Plan to determine that the company is required to perform internal and external vulnerability scans that are performed quarterly and annually. Observed the list of identified vulnerabilities to determine that the company uses GitHub, which is configured on Vanta, to perform host-based vulnerability scans on all external-facing systems. Observed the history of remediated vulnerabilities to determine that critical and high vulnerabilities are tracked to remediation. Inspected the tracking data to determine that the records of security issues are tracked on GitHub.	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.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed.	Inspected the Risk Management Policy to determine that the company is required to perform a formal risk assessment at least annually. Inspected a snapshot of the risk register, dated July 31, 2023, which shows risk scenarios, scores, and treatment plans to determine that the company is required to identify and mitigate risks that hinder the achievement of its business objectives.	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.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the company's Core Engineering Processes to determine that the company has established a change management process including the steps of testing, reviewing, obtaining approvals, and developing software. Observed that all relevant GitHub repositories are set to private. Observed code review process to determine that Chronicled requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring	The company's formal policies outline the requirements for the	Inspected the System and Security Monitoring to determine that vulnerability management and system monitoring procedures have been	No exceptions noted.

	procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	following functions related to IT / Engineering: - vulnerability management; - system monitoring.	documented by the company, mentioning that the recognized third-party security companies are required to evaluate the severity of vulnerabilities.	
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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Risk Management Plan to determine that the company is required to perform internal and external vulnerability scans that are performed quarterly and annually. Observed the list of identified vulnerabilities to determine that the company uses GitHub, which is configured on Vanta, to perform host-based vulnerability scans on all external-facing systems. Observed the history of remediated vulnerabilities to determine that critical and high vulnerabilities are tracked to remediation. Inspected the tracking data to determine that the records of security issues are tracked on GitHub.	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.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the computer inventory to determine that employee computers are monitored with the Vanta agent. Inspected the report of account block warning dated July 10, 2023, to determine that the company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches. Observed that GCP Cloud IDS is enabled on all networks and all projects have notifications configured for GCP Cloud IDS threat detections.	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	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Observed screenshots of Grafana and Slack to determine that an infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	No exceptions noted.

	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.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the cloud infrastructure data that GitHub, G Suite Admin, Jira, Confluence, CustomerCheckr, GCP, and Slack infrastructures are linked to Vanta to determine that activities on these applications are tracked on Vanta. Inspected the GCP resources data that all GCP subnets have VPC flow logs enabled, all GCP log sinks, storage buckets, pub/sub-topics, and BigQuery datasets are known to Vanta, logs are centrally stored in GCP, and retained for 365 days, and only authorized users can access tracked GCP log sinks to only authorized users to determine that log management is utilized.	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.	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the System and Security Monitoring to determine that vulnerability management and system monitoring procedures have been documented by the company, mentioning that the recognized third-party security companies are required to evaluate the severity of vulnerabilities.	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.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the Penetration Test report provided by IOActive on November 2, 2022 to determine that a penetration test is performed at least annually, but is not due to be performed during the observation window.	No performance.
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	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the record of security issues to determine that security issues are labelled, tracked, prioritized, and assigned owners in GitHub and Jira, and all tasks in GitHub and Jira labelled with security, p1, and p2 tags are marked as complete.	No exceptions noted.

	whether they represent security events.			
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 company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the Incident Response Plan to determine that an incident response procedure has been defined that the company expects to be followed in response to an incident. Inspected the policy acceptance data to determine that all employees have accepted the Incident Response Plan. Inspected the issues that all GitHub and Jira tasks labelled with security, p1 and p2 are marked as complete.	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 company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Information Security Incident Response to determine that the incident response procedure and roles and responsibilities of response team members to report, resolve, and document security and privacy incidents have been documented. Inspected the policy acceptance data to determine that all employees have acknowledged the Information Security Incident Response.	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.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the record of security issues to determine that security issues are labelled, tracked, prioritized, and assigned owners in GitHub and Jira, and all tasks in GitHub and Jira labelled with security, p1, and p2 tags are marked as complete.	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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Risk Management Plan to determine that the company is required to perform internal and external vulnerability scans that are performed quarterly and annually. Observed the list of identified vulnerabilities to determine that the company uses GitHub, which is configured on Vanta, to perform host-based vulnerability scans on all external-facing systems. Observed the history of remediated vulnerabilities to determine that critical and high vulnerabilities are tracked to remediation. Inspected the tracking data to determine that	No exceptions noted.

			the records of security issues are tracked on GitHub.	
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.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Information Security Incident Response to determine that the incident response procedure and roles and responsibilities of response team members to report, resolve, and document security and privacy incidents have been documented. Inspected the policy acceptance data to determine that all employees have acknowledged the Information Security Incident Response.	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.	The company tests their incident response plan at least annually.	Inspected an Incident Response Test dated February 15, 2023, to determine that the company tests the incident response plan at least annually and develops a remediation plan.	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.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the Incident Response Plan to determine that an incident response procedure has been defined that the company expects to be followed in response to an incident. Inspected the policy acceptance data to determine that all employees have accepted the Incident Response Plan. Inspected the issues that all GitHub and Jira tasks labelled with security, p1 and p2 are marked as complete.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company tests their incident response plan at least annually.	Inspected an Incident Response Test dated February 15, 2023, to determine that the company tests the incident response plan at least annually and develops a remediation plan.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the Incident Response Plan to determine that an incident response procedure has been defined that the company expects to be followed in response to an incident. Inspected the policy acceptance data to determine that all employees have accepted the Incident Response Plan. Inspected the issues that all GitHub and Jira tasks labelled with security, p1 and p2 are marked as complete.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to	The company has security and privacy incident response	Inspected the Information Security Incident Response to determine that the incident response procedure and roles and	No exceptions noted.

	recover from identified security incidents.	policies and procedures that are documented and communicated to authorized users.	responsibilities of response team members to report, resolve, and document security and privacy incidents have been documented. Inspected the policy acceptance data to determine that all employees have acknowledged the Information Security Incident Response.	
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery Plan to determine that a disaster recovery test is required to be performed on an annual basis. Inspected the policy acceptance data to determine that all employees have agreed to the Business Continuity and Disaster Recovery Plan. Inspected the details of the recovery test scenario which was performed on July 19, 2023, to determine that the company tests the BC/DR at least 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.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the company's Core Engineering Processes to determine that the company has established a change management process including the steps of testing, reviewing, obtaining approvals, and developing software. Observed that all relevant GitHub repositories are set to private. Observed code review process to determine that Chronicled requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	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.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the record of security issues to determine that security issues are labelled, tracked, prioritized, and assigned owners in GitHub and Jira, and all tasks in GitHub and Jira labelled with security, p1, and p2 tags are marked as complete.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high	Inspected the Risk Management Plan to determine that the company is required to perform internal and external vulnerability scans that are performed quarterly and annually.	No exceptions noted.

	infrastructure, data, software, and procedures to meet its objectives.	vulnerabilities are tracked to remediation.	Observed the list of identified vulnerabilities to determine that the company uses GitHub, which is configured on Vanta, to perform host-based vulnerability scans on all external-facing systems. Observed the history of remediated vulnerabilities to determine that critical and high vulnerabilities are tracked to remediation. Inspected the tracking data to determine that the records of security issues are tracked on GitHub.	
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.	The company restricts access to migrate changes to production to authorized personnel.	Inspected the version control system data showing that the company uses GitHub as a version control system and the visibility of all relevant GitHub repositories has been set to private to determine that the company restricts access to migrate changes to production to authorized personnel.	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.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the Penetration Test report provided by IOActive on November 2, 2022 to determine that a penetration test is performed at least annually, but is not due to be performed during the observation window.	No performance.
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.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Third Party Management Policy to determine that the company requires third parties to maintain a secure development program consistent with industry software and systems development best practices including risk assessment, formal change management, code standards, code review, and testing. Inspected the company's Core Engineering Processes to determine that the company has established a change management process including the steps of testing, reviewing, and developing software.	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.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the system export data to determine that all GCP Compute Instances are associated with a GCP network. Observed the company's GCP firewall ules to determine that firewalls are configured to prevent unauthorized access. Observed the ingress port review via GitHub to	No exceptions noted.

			determine that the company reviews its firewall rulesets at least annually. Observed the list of users with encryption key access to determine that the company restricts encryption key access to authorized users. Observed an access approval ticket to determine that the company has procedures in place to ensure that access is granted based on role.	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed.	Inspected the Risk Management Policy to determine that the company is required to perform a formal risk assessment at least annually. Inspected a snapshot of the risk register, dated July 31, 2023, which shows risk scenarios, scores, and treatment plans to determine that the company is required to identify and mitigate risks that hinder the achievement of its business objectives.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the roles and responsibilities have been established to execute the communication plan and strategy for the continuity of critical services. Inspected the policy acceptance to determine that all employees have acknowledged the Business Continuity and Disaster Recovery Plan.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected a cybersecurity insurance policy to determine that Chronicled maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated	The company has written agreements in place with vendors and related	Inspected the Third-Party Management Policy to determine that the company requires agreements to be signed with vendors to	No exceptions noted.

	with vendors and business partners.	third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	acknowledge their confidentiality, integrity, availability, and privacy commitments. Observed the vendor inventory to determine that the company has maintained a list of vendors along with their risk levels. Inspected the GCP Terms of service to determine that the confidentiality and privacy commitments of the vendors are documented. Inspected the company's Privacy Policy to determine that privacy, security, and service commitments have been communicated to vendors through the publicly available website.	
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the Third Party Management Policy to determine that the third-party risk management, security standards, and vendors' service review and monitoring requirements have been described. Observed the vendor inventory to determine that the company has maintained a list of vendors along with their risk levels. Inspected the vendor directory to determine that the company has a compliance security report for Google Workspace; all other vendors are low/medium risk.	No exceptions noted.