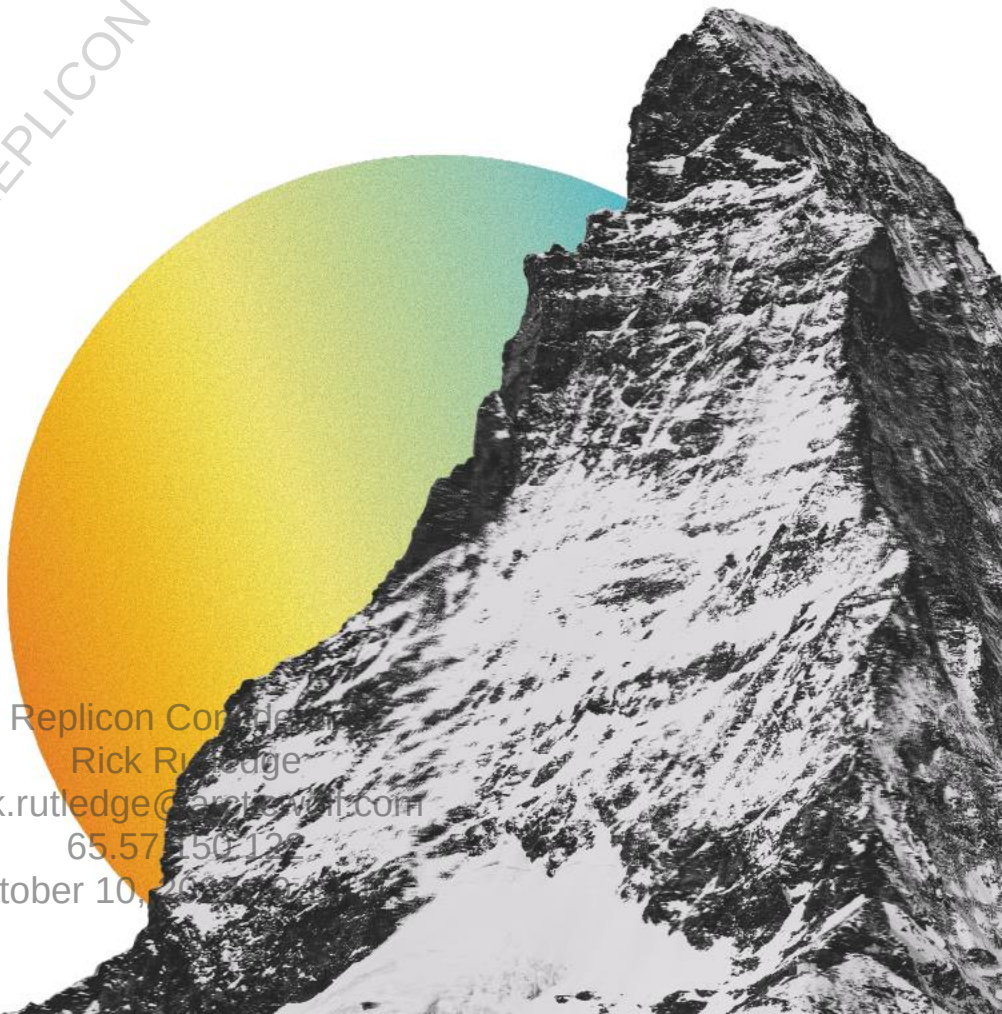
A-LIGN

Replicon Inc.

Type 2 SOC 1

2022

REPLICON™ The Time Intelligence Company



REPORT ON MANAGEMENT'S DESCRIPTION OF REPLICON INC.'S SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

Pursuant to Statement on Standards for Attestation Engagements No. 18 (SSAE 18) Type 2

October 1, 2021 to April 30, 2022

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

Table of Contents

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

SECTION 1

ASSERTION OF REPLICON INC.'S MANAGEMENT

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

Assertion of Replicon Inc.'s Management

May 16, 2022

We have prepared the description of Replicon Inc.'s ('Replicon' or 'the Company') information technology general control system for the Replicon Cloud Platform Services System entitled "Description of Replicon Inc.'s Cloud Platform Services System" throughout the period October 1, 2021 to April 30, 2022, (description) for user entities of the system during some or all of the period October 1, 2021 to April 30, 2022, and their user auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

Replicon uses Amazon Web Services ('AWS' or 'subservice organization') for cloud hosting services. The description includes only the control objectives and related controls of Replicon and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by Replicon in the description can be achieved only if complementary subservice organization controls assumed in the design of Replicon's controls are suitably designed and operating effectively, along with the related controls at Replicon. The description does not extend to controls of the subservice organization.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Replicon controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

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

a. The description fairly presents the information technology general control system made available to user entities of the system during some or all of the period October 1, 2021 to April 30, 2022 as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

   i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including:

      (1) the types of services provided.

      (2) the procedures, within both automated and manual systems, by which services are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities.

      (3) how the system captures significant events and conditions, other than transactions.

      (4) the process used to prepare reports and other information for user entities.

      (5) services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.

      (6) the specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of the service organization's controls.

(7) other aspects of our control environment, risk assessment process, information and communication systems (including related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

ii. includes relevant details of changes to the service organization's system during the period covered by the description.

iii. does not omit or distort information relevant to the scope of the information technology general control system, while acknowledging that the description is prepared to meet the common needs of broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Replicon Cloud Platform Services information technology general control system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period October 1, 2021 to April 30, 2022, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of Replicon's controls throughout the period October 1, 2021 to April 30, 2022. The criteria we used in making this assertion were that:

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;

ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Neal Alberda
Vice President, Information Systems and Technology
Replicon Inc.

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Replicon Inc.

Scope

We have examined Replicon's description of its information technology general control system for the Replicon Cloud Platform Services entitled "Description of Replicon Inc.'s Cloud Platform Services System" throughout the period October 1, 2021 to April 30, 2022, (description) and the suitability of the design and operating effectiveness of Replicon's controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Assertion of Replicon Inc.'s Management" (assertion).

Replicon uses AWS for cloud hosting services. The description includes only the control objectives and related controls of Replicon and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by Replicon can be achieved only if complementary subservice organization controls assumed in the design of Replicon are suitably designed and operating effectively, along with the related controls at Replicon. Our examination did not extend to controls of 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 control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of Replicon's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design and operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section 1 of this report, Replicon has provided their assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Replicon is responsible for preparing the description and their assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2021 to April 30, 2022. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

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

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved
- Evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization in their assertion

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements, and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in its information technology general control system. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become inadequate or fail.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in Replicon's assertion:

a. the description fairly presents the information technology general control system that was designed and implemented throughout the period October 1, 2021 to April 30, 2022.
b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2021 to April 30, 2022 and subservice organizations and user entities applied the complementary user entity controls contemplated in the design of Replicon's controls throughout the period October 1, 2021 to April 30, 2022.
c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2021 to April 30, 2022, if complementary subservice organization and user entity controls assume in the design of Replicon's controls operated effectively throughout the period October 1, 2021 to April 30, 2022.

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4 is intended solely for the information and use of Replicon, user entities of Replicon's information technology general control system during some or all of the period October 1, 2021 to April 30, 2022, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
May 16, 2022

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

SECTION 3

DESCRIPTION OF REPLICON INC.'S CLOUD PLATFORM SERVICES SYSTEM

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

OVERVIEW OF OPERATIONS

Company Background

Replicon was founded in 1996 and provides time tracking solutions for corporations. Replicon has multiple client industries that utilize Replicon's time and expense tracking product suite to track time and expenses to manage projects, bill clients, and automate time and attendance policies within one end-to-end solution.

Replicon is a privately held company with head office operations based in Calgary, Alberta, and additional offices located in Toronto, Ontario; Redwood City, California; Bangalore, India; London, England; and Sydney, Australia. The company currently employs approximately 700 people.

Description of Services Provided

The following products form the Replicon Cloud Platform (Gen 3) can be deployed individually, or as an integrated suite:

- Polaris
- TimeBill
- TimeBill Quickstart
- TimeBill Plus
- TimeCost
- TimeCost Plus
- TimeAttend
- TimeAttend QuickStart
- TimeAttend Plus
- TimeOff
- TimeOff Plus
- TimeOff Enterprise
- Expense
- Expense QuickStart
- Expense Plus
- Time Intelligence
- Professional Services Automation
- Project Portfolio Management
- ProjectTime
- ProjectTime Plus
- Workforce Management

Through a transparent implementation, clients will not have to maintain the product. This enables organizations to manage individual time at the department or corporate level. Whether it is one or the entire product suite, the Replicon Cloud Platform allows for the client to configure the application as desired for their business needs.

Users can configure how the system works for their business requirements such as timesheet periods, preferred e-mail notifications, and timesheet format. Users can also configure authentication settings, password parameters, and other settings such as specifying an automatic idle session timeout, using a secure browser connection, or enabling hierarchy filtering. These preferences are applied to the entire system as opposed to specific individuals or particular groups of users. Some of the password security settings include alphanumeric requirements, additional special characters, minimum password length, and password expiration intervals.

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

The Replicon Cloud Platform includes hosting the software product and related data allowing the client to access the system through the Internet 24 hours per day. Replicon's on-site and remote backup operations are designed to ensure the continuity and availability of the Replicon Cloud Platform system and production data.

The Replicon Cloud Platform is built with high availability systems and network devices on secured and redundant infrastructure. This Software-as-a-Service (SaaS) solution runs on servers hosted within AWS, across four regions, six availability zones, and two additional regions for disaster recovery.

Replicon Cloud Platform feature enhancements and defects are performed under quality control procedures in accordance with Replicon's change management process to help ensure system availability and client satisfaction.

Replicon allows users to create highly customized reports to assist with tracking and managing time, expenses, projects, and users. Reports can be viewed within the application or saved to a portable document format (PDF) or spreadsheet (CSV) document. Additionally, reports can be sent via e-mail according to predefined schedules. The reporting feature offers a wide number of options for report configuration including the following:

- Fields and filters
- Data grouping and sorting
- Indicating whether summaries should be generated

Users can also add a new report based on available report templates. Once a report exists, it can be edited. These reports can be created as either public or private reports. Public reports are available to those users assigned a permission in which the report is enabled, whereas private reports are only available to the user who created them.

The Replicon Cloud Platform environment is an information technology general control (ITGC) system, and user entities are responsible for the procedures, by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information presented to them. Additionally, user entities are responsible for the procedures and controls governing the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions processed within the Replicon Cloud Platform. This includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

Significant Events

Replicon has implemented automated and manual procedures to capture and address significant events and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the Replicon Cloud Platform Services System. Please see the procedures, monitoring, and risk assessment procedures described in the relevant sections of this report for further details.

Functional Areas of Operation

The Replicon staff provides support for the above services in each of the following functional areas:

- Executive management - provides general oversight and strategic planning of operations
- IT operations - manages, monitors, and supports information and systems for operational effectiveness, integrity, availability, problem management, change management, and compliance while protecting systems from unauthorized access and misuse
- Development team - responsible for developing and testing application changes and providing technical support services to the information technology (IT) operations team for the Replicon Cloud Platform system

Boundaries of the System

The scope of this report includes the Replicon Cloud Platform Services System performed in the Calgary, Alberta; Toronto, Ontario; Redwood City, California; Bangalore, India; London, England; and Sydney, Australia facilities.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at various facilities.

Subservice Description of Services

Replicon utilizes AWS to host its various production environments.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by AWS to provide additional assurance that the control objectives described within this report are met:

Subservice Organization - AWS	
Control Objective	**Control**
Control Objective 2: Data Communications	Network devices are configured by AWS to only allow access to specific ports on other server systems within AWS S3.
	External data access is logged with the following information: data accessor Internet protocol (IP) address, object and operation. Logs are retained for at least 90 days.
	S3 generates and stores a one-way salted Hash-based Message Authentication Code (HMAC) of the customer encryption key. This salted HMAC value is not logged.
	Requests in key management services (KMS) are logged in AWS CloudTrail.
	Customer master keys used for cryptographic operations in KMS are logically secured so that no single AWS employee can gain access to the key material.
	AWS Services that integrate with AWS KMS for key management use a 256-bit data key locally to protect customer content.
	The key provided by KMS to integrated services is a 256-bit key and is encrypted with a 256-bit (advanced encryption standard) Advanced Encryption Standard (AES) master key unique to the customer's AWS account.
	Physical access to data centers is approved by an authorized individual.

Subservice Organization - AWS	
Control Objective	**Control**
	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
	Closed circuit television (CCTV) is used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
	Access to server locations is managed by electronic access control devices.
	AWS production media is securely decommissioned and physically destroyed prior to leaving AWS Secure Zones.
	AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable.
	AWS retains customer content per customer agreements.
	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
	AWS contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. The AWS contingency plan is tested on at least an annual basis.

Replicon management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant control objectives through written contracts, such as service level agreements. In addition, Replicon performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

Significant Changes in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Replicon's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Replicon's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook
- Background checks are performed for employees as a component of the hiring process

Commitment to Competence

Replicon's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements
- Training is provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

Replicon's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole

Organizational Structure and Assignment of Authority and Responsibility

Replicon's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Replicon's management believes that establishing an organizational structure includes considering key areas of authority and responsibility and lines of reporting. Replicon has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Replicon's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority, responsibility, and lines of reporting to personnel. These charts are communicated to employees and updated as needed.

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

Human Resources Policies and Practices

Replicon's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensures the service organization is operating at maximum efficiency. Replicon's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- Logical access to systems is approved and granted to an employee as a component of the hiring process
- Logical access to systems is revoked as a component of the termination process

RISK ASSESSMENT

Replicon's risk assessment process identifies and manages risks that could potentially affect Replicon's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Replicon identifies the underlying sources of risk, measures the impact to the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Replicon, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

Replicon has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Replicon attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, Replicon has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of those objectives.

Selection and Development of Control Activities Specified by the Service Organization

Control activities are a part of the process by which Replicon strives to achieve its business objectives. Replicon has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, control activities are established to meet the overall objectives of the organization.

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

The establishment of control activities is inclusive of general control activities over technology. The management personnel of Replicon evaluate the relationships between business processes and the use of technology to perform those processes to determine the dependencies on technology. The security management processes for the technology, along with other factors, are analyzed to define and establish the necessary control activities to achieve control objectives that include technology.

The establishment of the control activities is enforced by defined policies and procedures that specifically state management's directives for Replicon personnel. The policies serve as the rules that personnel follow when implementing certain control activities. The procedures are the series of steps the personnel should follow when performing business or technology processes and the control activities that are components of those processes. After the policies, procedures, and control activities are all established, each are implemented, monitored, reviewed, and improved when necessary.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices, adjacent to the service organization's description of control activities. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Computer Operations

Replicon maintains policies and procedures to guide Cloud Operations personnel in data backup and replication processes. Replicon utilizes AWS S3 to manage and maintain the production data supporting the Replicon Cloud Platform system. Data stored within AWS S3 includes cross-region replication which automatically replicates the data across different AWS regions. AWS S3 refers to full backups as snapshots.

AWS has built-in redundancies for the snapshot/backup data as the data is deployed using availability zones. If one availability zone were to fail, AWS has built-in redundancy to another zone within the same or different region. Therefore, snapshot/backup data is maintained separately from production.

As part of normal Cloud Operations, Cloud Operations personnel perform restores of production data on a regular basis, and the AWS system maintains an inventory of backup data for restoration purposes. The ability to access backup and replicated data within AWS is restricted to authorized members of the Cloud Operations team.

System Availability

Cloud Operations personnel maintain policies and procedures to guide personnel in performing AWS instance builds, patch management, and incident management in the production environment. The production network is configured with failover processes and redundant architecture that is inherent within the AWS management console to mitigate the risk of the disruption of business operations.

An environmental monitoring system is in place to monitor the availability and performance of the production servers and network devices. The system is configured to send automated e-mail alerts to Cloud Operations personnel when pre-defined thresholds are exceeded. Upon receipt of an alert, Cloud Operations personnel investigate the issue and determine what actions are required to resolve the issue.

Incident Management and Escalations

The Salesforce ticketing system is utilized for incident reporting and resolution. Incidents include the reporting of outages or bugs by customers and are assigned to operations personnel for resolution based on the incident severity, priority, and urgency. The Cloud Operations engineer monitors the status of incident tickets to ensure that production incidents are escalated, tracked, and addressed.

Information Security

Replicon has created information security policies and procedures to guide personnel in information security practices that include access control, remote access, information classification, information handling, incident response, and acceptable use. Upon notification of a user termination, Cloud Operations personnel remove system access to the production environment that includes the identification service, application, and database server operating systems, and databases.

Access Administration

Access to production systems is tracked and approved by the Associate Director of Cloud Operations prior to provisioning. For new hires with an applicable job role, the provisioning process starts with a new hire announcement from Human Resources to the Associate Director of Cloud Operations. The Associate Director of Cloud Operations approves and provisions user access accordingly and documents his approval in a user access provisioning spreadsheet. Access changes for existing personnel are also approved and tracked in the same manner to ensure that the access being provisioned is commensurate with job duties.

Access to system information is protected by authentication and authorization mechanisms. User authentication is required to access Replicon's production environment, including the application and database server operating systems, databases, AWS management console, and the Replicon Cloud Platform. The Cloud Operations department is responsible for assigning and maintaining access rights to the production environment.

In order to gain access to the production environment, users are required to authenticate to the AWS management console using the Okta single sign-on application. Authentication into the AWS management console via Okta, requires a username, password, and a multi-factor token generated via OneLogin. The Okta application is configured to enforce password requirements that include minimum length and password complexities. Once users authenticate to AWS, they have access to modify the production infrastructure and database schema.

Replicon Cloud Operations personnel have configured the AWS environment for auto-scaling that allows for continuous and automated deployment of application server and PostgreSQL database instances to meet resource demands. This allows for the production environment to automatically scale to the necessary level (adding and removing AWS instances) to meet resource demands without the manual dependency of Cloud Operations personnel.

For a user to access the production application server operating system, they are required to authenticate via Okta and be assigned to dedicated security groups. Group memberships are restricted to Cloud Operations team personnel. The ability to access and administer the AWS management console via the Okta tool is restricted to authorized Cloud Operations personnel.

Logging and Monitoring

The Cloud Operations department has configured the application and database server operating systems, databases, AWS management console, and the Replicon Cloud Platform to log user-related events, and Cloud Operations personnel monitor for event-related alerts on a continuous basis to determine if any irregular system-level activities have occurred. In the event that a member of Cloud Operations identifies an issue that requires resolution, the issue will be discussed with Cloud Operations management and relevant action plans will be documented.

Prior to a user being granted access to the Replicon Cloud Platform, they are required to enter a user account and password. The Replicon Cloud Platform is configured to require a minimum password length for user accounts. Replicon does not have administrative access to a customer's Replicon Cloud Platform. However, if a customer requires assistance from Replicon Cloud Operations, the customer will provide login information for temporary usage.

Data Communications

Security Groups

Replicon Cloud Operations personnel follow the AWS "best practices" guide to provide a network security framework for their production environment. AWS EC2 security groups are in place to provide perimeter security for the Replicon Cloud Platform environment. The security groups monitor incoming network traffic by analyzing the data packets and determining whether they should be allowed based on the ruleset. The ability to modify the security groups is restricted to authorized Cloud Operations personnel via the AWS management console. Cloud Operations personnel are required to authenticate to the AWS management console using a user account, password, and multi-factor authentication code in order to perform any modifications to the security groups. The AWS management console is configured to enforce password requirements that include minimum length and password complexities.

The production systems hosted by AWS are protected from unauthorized Internet traffic. The dynamic/private Transmission Control Protocol (TCP) is the only protocol open to filter unauthorized traffic. In addition, traffic trying to authorize against the AWS management console to access Replicon's production systems is required to authenticate with a user account, password, and a multi-factor authentication code. Administrative access to the AWS console is restricted to authorized Cloud Operations personnel.

Network Infrastructure Security

The Replicon Security Team will review a penetration test report as evidence that a third-party specialist performs a penetration test on the application on an annual basis. A security monitoring tool was utilized to analyze suspected network events and scan production instances for suspected vulnerabilities. The security monitoring tool generates e-mail alerts of suspected network events or vulnerabilities. The Cloud Operations personnel review the e-mails and plans any remedial actions necessary to address any significant findings. These remedial actions are documented within the Jira ticketing system and are assigned to an IT resource for monitoring through resolution.

Remote Access and Encryption

Remote access to the production environment is restricted through an encrypted virtual private network (VPN). The VPN is encrypted with the advanced encryption standard (AES) 256 encryption protocol. Before a user can establish a VPN connection, they are required to authenticate via a user account, password, and enter a multi-factor token generated via OneLogin. Administrative access privileges within the VPN network are restricted to authorized IT personnel. Transport layer security (TLS) encryption is utilized for customer web sessions when accessing the Replicon Cloud Platform.

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

Application Change Control

Replicon has implemented policies and procedures to guide personnel in application development, maintenance, and documentation of application changes. Application change management activities are documented within a change management ticketing system. The Replicon application change process consists of application releases that are performed on an as-needed basis which could result in multiple releases per day. Each release consists of feature requests and defect requests that support the Replicon Cloud Platform. The application change process is separated into multiple change categories, and each type of change requires individual steps to be completed prior to the change being deployed into the production environment.

Feature Requests

A feature request is the implementation of a new feature to the existing Replicon Cloud Platform product. Due to feature requests being new application code within the application, various detailed steps and documentation items are required to be completed. A requirements analysis is completed by the Product Manager who is assigned to manage the deployment of the feature, and the requirements must be completed prior to the start of the feature design. The feature design documentation is completed in order to provide visual detail to support the developer's technical specifications for the new feature. Each of the aforementioned items is a key piece in the progression of the feature request and to ensure the feature was designed and executed according to the initial requirements.

Defect Requests

Defects are changes to the application code for an existing feature within the Replicon Cloud Platform. Application defects follow the normal change process and are combined into "Sprints/Epics" (groupings of changes applied to production). Due to application defects being combined into "Sprints/Epics," the testing and approvals for application defects are completed prior to the "Epic" being released into production.

Quality Assurance (QA)

Prior to a release being deployed to production, QA personnel complete a series of QA testing. The QA testing varies depending on the types of code changes (i.e., features and defects) being included within the application release, and the evidence to support the QA testing process is documented and stored by the QA department. Once the QA department completes their testing, the QA lead sends an e-mail to a mailbox that includes the required parties involved in the change process to notify them the QA testing is complete.

Release Management

Prior to a release being deployed into production, Cloud Operations personnel perform functional testing in a test environment to determine if the change would cause any negative impact to the Replicon Cloud Platform. Once the testing has been completed by the Cloud Operations team, the QA department performs an additional review to verify the application change is ready for deployment to production. The QA team lead notifies the same mailbox mentioned above within the QA testing process to provide final approval and authorization of the change to initiate the release deployment process.

Application development and testing efforts are performed in development and test environments that are logically separated from the production environment. Development personnel utilize the GitHub version control software to control access to source code and provide rollback capabilities for application changes. The ability to modify source code within the version control software is restricted to authorized development and engineering personnel.

Administrative access privileges within the version control system are restricted to authorized release management personnel. The release deployment process is managed by the Cloud Operations department, and the ability to implement changes into the production environment is restricted to authorized members of the Cloud Operations and Engineering teams.

File Integrity Monitoring (FIM)

IT and Cloud Operations personnel review alerts on a continuous basis as evidence that a third-party provides FIM services to monitor for changes to the production environment. For a change to be released to production, a new AWS instance and Amazon Machine Image (AMI) must be created and applied to the production environment within AWS. CloudTrail is configured to monitor and send e-mail alerts for AWS instance deployments and terminations. Upon notification of an AWS instance being created or terminated, a member of the Cloud Operations team reviews the change to determine what was changed and the reason for the change.

User Documentation

Due to the release deployment process being performed as needed, some releases may not contain features and defects that impact a customer. Release notes are documented on the Replicon website for customers to review for releases that are customer impacting. For the releases that do not have an impact to a customer, the notes are stored internally within the technical writing team as to why they were not required to be submitted for customer review.

MONITORING

Management monitors internal controls to ensure that they are operating as intended and that controls are modified as conditions change. Replicon's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Vendor management procedures have been defined to review the services provided by external providers. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Replicon's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon the results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Vendor Management

Management's close involvement in Replicon's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Replicon's personnel.

Replicon has defined the following activities to oversee controls performed by vendors that could impact the Replicon Cloud Platform Services System:

- Reviewing attestation reports over services provided by the vendors and the subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Reporting Deficiencies

Deficiencies in management's internal control system surface from many sources, including the company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure findings of internal control deficiencies are reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and makes the decision for addressing deficiencies based on whether the incident was isolated or requires a change in the company's procedures or personnel.

INFORMATION AND COMMUNICATION SYSTEMS

Information Systems

Replicon has implemented mechanisms to track and record operational data to make strategic decisions and ensure objectives are consistently achieved. Information gathered from systems enable Replicon to understand business trends in order to maximize efforts and provide optimal services.

Infrastructure

The primary infrastructure used to provide Replicon's Cloud Platform Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Hosting Provider	AWS	The Replicon Cloud Platform Services System is hosted and managed by AWS
Firewall	AWS Security Groups	Controls traffic flow between servers on the internal network and between the internal network and the Internet
Storage	AWS S3	Stores information securely for longer retention

Software

The primary software used to provide Replicon's Cloud Platform Services System includes the following:

Primary Software	
Software	**Purpose**
Cloud Platform (Gen 3) system	Replicon's time and expense tracking product suite

Communication Systems

Communication is an integral component of Replicon's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Replicon, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, company-wide meetings are held annually in each geographic location to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the company-wide meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Replicon personnel via e-mail messages.

COMPLEMENTARY USER ENTITY CONTROLS

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

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

Control Objective 1: Information Security

1. User entities are responsible for configuring the Replicon Cloud Platform application password parameters and complexity requirements settings.
2. User entities are responsible for administering Replicon Cloud Platform security access privileges.
3. User entities are responsible for ensuring the supervision, management, and control of the use of Replicon services by their personnel.
4. User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to or created by them for use with Replicon Cloud Platform.
5. User entities are responsible for removing terminated employees' access to the Replicon Cloud Platform in a timely manner.
6. User entities are responsible for maintaining their own system(s) of record.

Control Objective 2: Data Communications

7. User entities are responsible for defining an appropriate encryption methodology utilized in relation to Replicon's systems.
8. User entities are responsible for determining whether Replicon's security infrastructure is appropriate for its needs and notifying Replicon of any requested modifications.

Control Objective 3: Computer Operations

9. User entities are responsible for immediately notifying Replicon of any actual or suspected information security breaches, including compromised user accounts.

Control Objective 4: Application Change Control

10. User entities are responsible for obtaining release notes from the Replicon website.

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

SECTION 4

DESCRIPTION OF REPLICON INC.'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

GUIDANCE REGARDING DESCRIPTION OF REPLICON INC.'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

A-LIGN ASSURANCE's examination of the controls of Replicon was limited to the control objectives and related control activities specified by the management of Replicon and did not encompass all aspects of Replicon's operations or operations at user organizations. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 18 (SSAE 18).

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether a SSAE 18 report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the processing of the user organization's transactions;
- Understand the flow of significant transactions through the service organization;
- Determine whether the control objectives are relevant to the user organization's financial statement assertions;
- Determine whether the service organization's controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user organization's financial statements and determine whether they have been implemented.

Replicon Confidential
Rick Rutledge
rick.rutledge@arcticwolf.com
65.57.150.122
October 10, 2022 19:14UTC

CONTROL AREA 1 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	General		
1.1	Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring.	No exceptions noted.
1.2	Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the Information Security and Compliance Manager regarding new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Inspected the hiring procedures, user access listings and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
1.3	Logical access to systems is revoked as a component of the termination process.	Inquired of the Information Security and Compliance Manager regarding terminations to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		Inspected the termination procedures, user access listings and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
	Network		
1.4	Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

CONTROL AREA 1 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.5	Network administrative access is restricted to only authorized personnel.	Inquired of the Information Security and Compliance Manager regarding administrative access to determine that network administrative access was restricted to only authorized personnel.	No exceptions noted.
		Inspected the network administrator user listing and access rights to determine that network administrative access was restricted to only authorized personnel.	No exceptions noted.
1.6	Networks are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length • Complexity	Inspected the network password configurations to determine that networks were configured to enforce password requirements that included: • Password history • Password age (minimum and maximum) • Password length • Complexity	No exceptions noted.
1.7	Network users are authenticated via individually assigned user accounts and passwords.	Inquired of the Information Security and Compliance Manager regarding network authentication to determine that network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Inspected the Password Control Policy to determine that network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
1.8	Network account lockout configurations are in place that include: • Account lockout threshold	Inspected the network account lockout configurations to determine that network account lockout configurations were in place that included: • Account lockout threshold	No exceptions noted.

CONTROL AREA 1 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.9	Network audit logging configurations are in place that include: • Account logon events • Account management • Object access • System events	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Object access • System events	No exceptions noted.
1.10	Network audit logs are maintained and available for review, if needed.	Inquired of the Information Security and Compliance Manager regarding audit logs to determine that network audit logs were maintained and available for review, if needed.	No exceptions noted.
		Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logs were maintained and available for review, if needed.	No exceptions noted.
	Operating System (Application, Web, and Database Servers)		
1.11	Operating system user access is restricted via role-based security privileges defined within the access control system.	Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
1.12	Operating system administrative access is restricted to only authorized personnel.	Inquired of the Information Security and Compliance Manager regarding administrative access to determine that operating system administrative access was restricted to only authorized personnel.	No exceptions noted.
		Inspected the operating system administrator user listing and access rights to determine that operating system administrative access was restricted to only authorized personnel.	No exceptions noted.

CONTROL AREA 1 INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.13	Operating systems are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length • Complexity	Inspected the operating system password configurations to determine that operating systems were configured to enforce password requirements that included: • Password history • Password age (minimum and maximum) • Password length • Complexity	No exceptions noted.
1.14	Operating system users are authenticated via individually assigned user accounts and passwords.	Inquired of the Information Security and Compliance Manager regarding operating system authentication to determine that operating system users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Inspected the password control policy and access control policy to determine that operating system users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
1.15	Operating system account lockout configurations are in place that include: • Account lockout threshold	Inspected the operating system account lockout configurations to determine that operating system account lockout configurations were in place that included: • Account lockout threshold	No exceptions noted.
1.16	Operating system audit logging configurations are in place that include: • Account logon events • System events	Inspected the operating system audit logging configurations and an example operating system audit log extract to determine that operating system audit logging configurations were in place that included: • Account logon events • System events	No exceptions noted.

CONTROL AREA 1 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.17	Operating system audit logs are maintained and available for review, if needed.	Inquired of the Information Security and Compliance Manager regarding audit logs to determine that operating system audit logs were maintained and available for review, if needed.	No exceptions noted.
		Inspected the operating system audit logging configurations and an example operating system audit log extract to determine that operating system audit logs were maintained and available for review, if needed.	No exceptions noted.
	Database		
1.18	Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
1.19	Database administrative access is restricted to only authorized personnel.	Inquired of the Information Security and Compliance Manager regarding administrative access to determine that database administrative access was restricted to only authorized personnel.	No exceptions noted.
		Inspected the database administrator user listing and access rights to determine that database administrative access was restricted to only authorized personnel.	No exceptions noted.
1.20	Databases are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length • Complexity	Inspected the database password configurations to determine that database was configured to enforce password requirements that included: • Password history • Password age (minimum and maximum) • Password length • Complexity	No exceptions noted.

CONTROL AREA 1 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.21	Database users are authenticated via individually assigned user accounts and passwords.	Inquired of the Information Security and Compliance Manager regarding database authentication to determine that database users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Inspected the Password Control Policy to determine that database users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
1.22	Database audit logging configurations are in place that include: • Account logon events • Object access • System events	Inspected the database audit logging configurations and an example database audit log extract to determine that database audit logging configurations were in place that included: • Account logon events • Object access • System events	No exceptions noted.
1.23	Database audit logs are maintained and available for review, if needed.	Inquired of the Information Security and Compliance Manager regarding audit logs to determine the database audit logs were maintained and available for review, if needed.	No exceptions noted.
		Inspected the database audit logging configurations and an example database audit log extract to determine that database audit logs were maintained and available for review, if needed.	No exceptions noted.
	Application		
1.24	Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

CONTROL AREA 1 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.25	Application administrative access is restricted to only authorized personnel.	Inquired of the Information Security and Compliance Manager regarding administrative access to determine that application administrative access was restricted to only authorized personnel.	No exceptions noted.
		Inspected the application administrator user listing and access rights to determine that application administrative access was restricted to only authorized personnel.	No exceptions noted.
1.26	The application is configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length • Complexity	Inspected the application password configurations to determine that application was configured to enforce password requirements that included: • Password history • Password age (minimum and maximum) • Password length • Complexity	No exceptions noted.
1.27	Application users are authenticated via individually assigned user accounts and passwords.	Inquired of the Information Security and Compliance Manager regarding application authentication to determine that application users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Inspected the Password Control Policy to determine that application users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
1.28	Application account lockout configurations are in place that include: • Account lockout threshold	Inspected the application account lockout configurations to determine that application account lockout configurations were in place that included: • Account lockout threshold	No exceptions noted.

CONTROL AREA 1 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.29	Application audit policy configurations are in place.	Inspected the application audit logging configurations and an example application audit log extract to determine that application audit logging configurations were in place.	No exceptions noted.
1.30	Application audit logs are maintained and available for review, if needed.	Inquired of the Information Security and Compliance Manager regarding audit logs to determine that application audit logs were maintained and available for review, if needed.	No exceptions noted.
		Inspected the application audit logging configurations and an example application audit log extract to determine that application audit logs were maintained and available for review, if needed.	No exceptions noted.
	Remote Access		
1.31	VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
1.32	The ability to administer VPN access is restricted to only authorized personnel.	Inquired of the Information Security and Compliance Manager regarding VPN access to determine that the ability to administer VPN access was restricted to only authorized personnel.	No exceptions noted.
		Inspected the VPN administrator user listing to determine that the ability to administer VPN access was restricted to only authorized personnel.	No exceptions noted.

CONTROL AREA 1 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.33	VPN users are authenticated via multi-factor authentication prior to being granted remote access to the system.	Inquired of the Information Security and Compliance Manager regarding VPN authentication to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system. Inspected the VPN authentication configurations to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted. No exceptions noted.

CONTROL AREA 2 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data transmissions between the service organization and its clients are complete, accurate, and secure and that data received is posted to the relevant systems in accordance with the Company's guidelines.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	Network address translation (NAT) functionality is utilized to manage internal IP addresses.	Inspected NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
2.2	VPN and TLS technologies are used for defined points of connectivity.	Inspected TLS configurations, VPN authentication configurations and digital certificates to determine that VPN and TLS technologies were used for defined points of connectivity.	No exceptions noted.
2.3	VPN users are authenticated via multi-factor authentication prior to being granted remote access to the system.	Inquired of the Information Security and Compliance Manager regarding VPN authentication to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
		Inspected the VPN authentication configurations to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
2.4	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected TLS encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
2.5	Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
2.6	Critical data is stored in encrypted format using AES.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES.	No exceptions noted.

CONTROL AREA 2 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data transmissions between the service organization and its clients are complete, accurate, and secure and that data received is posted to the relevant systems in accordance with the Company's guidelines.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.7	Backup media is stored in an encrypted format.	Inspected the encryption configuration for backup media to determine that backup media was stored in an encrypted format.	No exceptions noted.
2.8	VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
2.9	Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the Information Security and Compliance Manager regarding VPN authentication to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
2.10	Logical access to stored data is restricted to authorized personnel.	Inquired of the Information Security and Compliance Manager regarding access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
2.11	A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		Inspected the firewall rule set for a sample of production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.

CONTROL AREA 2 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data transmissions between the service organization and its clients are complete, accurate, and secure and that data received is posted to the relevant systems in accordance with the Company's guidelines.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.12	The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and the firewall rule set for a sample of production servers to determine the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
2.13	An intrusion detection system (IPS) is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram and IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		Inspected IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
2.14	The IPS is configured to notify personnel upon intrusion detection.	Inspected an example IPS log extract and alert notification to determine that the IPS was configured to notify personnel upon intrusion detection.	No exceptions noted.
2.15	Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
2.16	The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
2.17	The antivirus software is configured to scan workstations weekly.	Inspected the antivirus configurations to determine that the antivirus software was configured to scan workstations weekly.	No exceptions noted.

CONTROL AREA 2 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data transmissions between the service organization and its clients are complete, accurate, and secure and that data received is posted to the relevant systems in accordance with the Company's guidelines.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.18	Critical data is stored in encrypted format using AES.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES.	No exceptions noted.
2.19	A demilitarized zone (DMZ) is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ configurations to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.

CONTROL AREA 3 **COMPUTER OPERATIONS - AVAILABILITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system processing is authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IPS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
3.2	The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example alert generated from the FIM software, and an example IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
3.3	Processing capacity is monitored 24x7x365.	Inspected the monitoring tool configurations to determine that processing capacity was monitored 24x7x365.	No exceptions noted.
3.4	Future processing demand is forecasted and compared to scheduled capacity on an annual basis.	Inspected the annual future processing capacity demand forecast to determine that future processing demand was forecasted and compared to scheduled capacity on an annual basis.	No exceptions noted.
3.5	Future processing demand forecasts are managed through auto-scaling software.	Inspected AWS auto-scaling configurations to determine that future processing demand forecasts were managed through auto-scaling software.	No exceptions noted.
3.6	The change management process is followed when a change is made to a system.	Inspected the supporting ticket for a sample of changes made to a system to determine that the change management process was followed when a change was made to a system.	No exceptions noted.

CONTROL AREA 3 **COMPUTER OPERATIONS - AVAILABILITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system processing is authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.7	Redundant architecture is in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	Inspected the disaster recovery plan and network diagram to determine that redundant architecture was in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	No exceptions noted.
3.8	A disaster recovery plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.	Inspected the disaster recovery plan to determine that a business continuity plan was documented and in place that outlined the range of disaster scenarios and steps the business would take in a disaster to ensure the timely resumption of critical business operations.	No exceptions noted.
3.9	The disaster recovery plan is tested on a monthly basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	Inspected the completed disaster recovery test results for a sample of months to determine that the business continuity plan was tested on a monthly basis and included: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	No exceptions noted.

CONTROL AREA 4 **APPLICATION CHANGE CONTROL**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that new development of and changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transaction processing.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.1	Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
4.2	System changes are communicated to both affected internal and external users.	Inspected an example newsletter to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.
4.3	Access to implement changes in the production environment is restricted to authorized IT personnel.	Inquired of the Information Security and Compliance Manager regarding access to implement changes to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
		Inspected the list of users with access to deploy changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
4.4	System changes are authorized and approved by management prior to implementation.	Inquired of the Information Security and Compliance Manager regarding access to approve changes to determine that system changes were authorized and approved by management prior to implementation.	No exceptions noted.
		Inspected the supporting ticket for a sample of infrastructure changes and operating system changes to determine that system changes were authorized and approved by management prior to implementation.	No exceptions noted.
4.5	Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.	Inspected the change control software configurations to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed.	No exceptions noted.

CONTROL AREA 4 **APPLICATION CHANGE CONTROL**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that new development of and changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transaction processing.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.6	Development and test environments are physically and logically separated from the production environment.	Inspected the separate development and production environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.
4.7	System change requests are documented and tracked in a ticketing system.	Inspected the supporting ticket for a sample of infrastructure changes and operating system changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
4.8	FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected FIM configurations to determine that FIM software was in place to ensure only authorized changes were deployed into the production environment.	No exceptions noted.
4.9	System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.	Inspected the supporting ticket for a sample of infrastructure changes and operating system changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change.	No exceptions noted.
4.10	System changes implemented to the production environment are evaluated for impact to the entity's objectives.	Inspected the supporting ticket for a sample of infrastructure changes and operating system changes to determine that system changes implemented to the production environment were evaluated for impact to the entity's objectives.	No exceptions noted.
4.11	System changes implemented for remediating incidents follow the standard change management process.	Inspected the change management policies and procedures to determine that system changes implemented for remediating incidents followed the standard change management process.	No exceptions noted.

CONTROL AREA 4 **APPLICATION CHANGE CONTROL**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that new development of and changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transaction processing.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.12	Information security policies and procedures document the baseline requirements for configuration of IT systems and tools.	Inspected the information security policies and procedures to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools.	No exceptions noted.
4.13	Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.	No exceptions noted.