Clear21 Pty Ltd

Type 2 SOC 3

2022

A-LIGN.COM

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

December 1, 2021 to November 30, 2022

Table of Contents

SECTION 1

ASSERTION OF CLEAR21 PTY LTD MANAGEMENT

ASSERTION OF CLEAR21 PTY LTD MANAGEMENT

December 15, 2022

We are responsible for designing, implementing, operating, and maintaining effective controls within Clear21 Pty Ltd's ('Clear21' or 'the Company') Software as a Service System throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that Clear21's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Clear21 Pty Ltd's Description of Its Software as a Service System throughout the period December 1, 2021 to November 30, 2022" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that Clear21's service commitments and system requirements were achieved based on the trust services criteria. Clear21's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Clear21 Pty Ltd's Description of Its Software as a Service System throughout the period December 1, 2021 to November 30, 2022".

Clear21 uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Clear21, to achieve Clear21's service commitments and system requirements based on the applicable trust services criteria. The description presents Clear21's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Clear21's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Clear21's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Clear21's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period December 1, 2021 to November 30, 2022 to provide reasonable assurance that Clear21's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Clear21's controls operated effectively throughout that period.

Glendon Smith
Chief Operating Officer
Clear21 Pty Ltd

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Clear21 Pty Ltd:

Scope

We have examined Clear21 Pty Ltd's ('Clear21' or 'the Company') accompanying assertion titled "Assertion of Clear21 Pty Ltd Management" (assertion) that the controls within Clear21's Software as a Service System were effective throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that Clear21's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Clear21 uses AWS to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Clear21, to achieve Clear21's service commitments and system requirements based on the applicable trust services criteria. The description presents Clear21's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Clear21's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Clear21, to achieve Clear21's service commitments and system requirements based on the applicable trust services criteria. The description presents Clear21's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Clear21's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Clear21 is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Clear21's service commitments and system requirements were achieved. Clear21 has also provided the accompanying assertion (Clear21 assertion) about the effectiveness of controls within the system. When preparing its assertion, Clear21 is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization’s service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

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

Independence and Ethical Responsibilities

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

Inherent Limitations

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

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

Opinion

In our opinion, management’s assertion that the controls within Clear21’s Software as a Service System were suitably designed and operating effectively throughout the period December 1, 2021 to November 30, 2022, to provide reasonable assurance that Clear21’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Clear21’s controls operated effectively throughout that period.

The SOC logo for Service Organizations on Clear21’s website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Clear21, user entities of Clear21’s Software as a Service during some or all of the period December 1, 2021 to November 30, 2022, business partners of Clear21 subject to risks arising from interactions with the Software as a Service, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements.

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

A-LIGN ASSURANCE

Tampa, Florida
December 15, 2022

SECTION 3

CLEAR21 PTY LTD’S DESCRIPTION OF ITS SOFTWARE AS A SERVICE SYSTEM THROUGHOUT THE PERIOD DECEMBER 1, 2021 TO NOVEMBER 30, 2022

OVERVIEW OF OPERATIONS

Company Background

Clear21 is a software company dedicated to streamlining business processes via user-friendly, reliable, and cost-effective SaaS solutions. It strives to achieve measurable, sustainable improvements for Clear21 customers' business success and personal satisfaction.

Clear21 was founded in 1996, with a vision of developing superior integrated software solutions for the automotive repair industry.

In line with technological advances and industry trends, the company launched their premier iBodyshop SaaS product in 2015. It has since succeeded in becoming the market leader of this industry segment in Australia and New Zealand.

The company has diversified, launching several SaaS solutions based on the reliable, scalable, and secure Clear21 SaaS platform originally created for the iBodyshop product.

Industries served by Clear21 include Automotive Repair, Insurance & Manufacturing.

Description of Services Provided

Clear21 supports customers across Australia & New Zealand.

Clear21's products, iBodyshop, RepairConnection, Clear21 Assessing, Clear21 provides software services primarily to the Australia and New Zealand markets.

The Clear21 platform is a multi-user, multi-tenant, cloud-based application platform that hosts the Clear21 suite of end-user SaaS applications.

The following application service offerings are hosted on this platform:

iBodyshop

Designed to be a one-stop solution for medium to large panel repair shops, including:

- Estimating
- End-to-end job management
- Workshop management, scheduling and time recording
- Parts inventory
- Fully integrated accounting
- Connectivity with third-party assessing, accounting, and parts supply systems

RepairConnection

Provides a parts marketplace where suppliers can quote to supply parts to repairers.

Clear21 Assessing

Allows insurance claims assessors to assess and authorize insurance claims.

Principal Service Commitments and System Requirements

Clear21 has established processes, policies, and procedures to meet its objectives related to its iBodyshop system (the “System”). Those objectives are based on the purpose, vision, and values of Clear21 as well as commitments that Clear21 makes to user entities, the requirements of laws and regulations that apply to Clear21’s activities, and the operational requirements that Clear21 has established.

Commitments related to security, availability, and integrity of the System are documented, and communicated in customer agreements, as well as in public descriptions of the System. The operational requirements are communicated in Clear21’s processes, policies and procedures, system design documentation, and customer agreements. This includes policies around how the System is designed and developed, how the System is operated, how the system components are managed, and how employees are hired, developed, and managed to support the System.

Components of the System

Infrastructure

Clear21’s primary infrastructure used to provide the Software as a Service System includes the cloud hosted networking, compute, and database components of Amazon Web Services (AWS):

Primary Infrastructure		
System	**Type**	**Purpose**
Amazon Elastic Compute Cloud (EC2)	Cloud Compute	Secure and resizable compute capacity (virtual servers) in the cloud
AWS Lambda	Cloud Compute	Serverless, event-driven compute service
PostgreSQL	Data storage	Open-source relational database management system emphasizing extensibility and SQL compliance
Amazon Aurora	Data storage	Relational database service
Amazon Simple Storage Service (S3)	Data storage	Object, file, and block storage
AWS Network Firewall	Network Firewall	Managed service to deploy network protections for Amazon Virtual Private Clouds (VPCs)
AWS Elastic Load Balancing (ELB)	Networking	Automatically distributes incoming application traffic across multiple targets
AWS CloudFront	Content Delivery Network	Low-latency, global delivery of content
AWS Certificate Manager	Encryption	A service to provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services
AWS Key Management Service	Key Management	Centralized control over the cryptographic keys used to protect data

Software

Primary software used to support Clear21’s Software as a Service System includes the following:

Primary Software	
Software	**Purpose**
iBodyshop, RepairConnection, Clear21 Assessing	The software as a service product provided to Clear21 customers
AWS CloudTrail	Enables auditing, security monitoring, and operational troubleshooting by tracking user activity and API usage on AWS
AWS CloudWatch	Monitoring and management service that provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources
AWS GuardDuty	Threat detection service that continuously monitors AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation
GitHub	Source code repository used to manage the software code and version control
TeamCity	Continuous development/continuous integration software used to manage the pipeline of change release testing and deployment
1Password	Enterprise password manager used to store authentication secrets and strengthen password security
ESET	Anti-virus software used to protect endpoint devices from malware
Data Dog, Pingdom	System monitoring software used to log events and raise alerts to support system security and availability
Data Dog	Vulnerability scanning software to identify, log and resolve technical vulnerabilities
JIRA, Zendesk	Ticketing software used to log events and requirements to support the internal controls
ELMO	Human resources information system used to manage employee processes like onboarding, offboarding and performance
Data Dog	Security and compliance software used to monitor and manage the security, risk, and control activities to support compliance
Office 365	Microsoft’s suite of enterprise productivity, collaboration, and communication tools

People

Clear21 has 50 people that are organized into the following functional areas:

- Leadership: The executive level responsible for corporate governance
- Product: Responsible for managing the roadmap of requirements and balancing the Engineering team priorities
- Engineering: Responsible for building and maintaining the infrastructure and software
- Customer Success: Responsible for the customer experience, support, and services
- Implementations: Responsible for enterprise implementations and integrations to onboard and set up new customers

- Operations: Responsible for monitoring and supporting robust and effective company and system operations
- Risk and Compliance: Responsible for identification, assessment, treatment, and monitoring to manage risks and support compliance
- Partnerships: Responsible for managing partnerships with complementary service providers
- Sales: Responsible for onboarding new customers and aligning requirements
- Marketing: Responsible for branding, market positioning and attracting customers

Data

The data collected and processed by Clear21 includes the following types:

- Basic personal details: name, e-mail, contact details
- User activity: user activity within the software
- Financial account information: account balances, transactions
- Business information: proprietary data of business activities and property

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Clear21 policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Clear21 team member.

<u>Physical Security</u>

The critical infrastructure and data of the System are hosted by Amazon Web Services (AWS). There are no trusted local office networks. As such, Amazon Web Services (AWS) is responsible for the key physical security controls that support the System.

<u>Logical Access</u>

Clear21's logical access processes restrict access to the infrastructure, software, and data to only those that are authorized for access. Access is based on the concept of least privilege that limits the system components and access privileges to the minimum level required to fulfil job responsibilities.

The in-scope systems require approval and individual authentication practices prior to gaining access. Access management processes are followed to ensure new and modified access is approved, terminated users access is removed, and access rights are periodically reviewed and adjusted when no longer required. Additional information security policies and procedures require Clear21 employees to use the systems and data in an appropriate and authorized manner.

Automated and manual security practices are used to protect the perimeter security and network to prevent unauthorized access attempts and tampering from third-party actors with malicious intent. Those include applying encryption of data and communications, periodic testing for and remediation of technical vulnerabilities, and applying network controls like firewalls and event monitoring to prevent and detect unauthorized activity.

Clear21 employee workstations are required to follow defined security practices to mitigate the risks of data leakage and malware that may compromise the devices, system access and sensitive data.

System Operations

The System is monitored through a combination of automated and manual processes to prevent and detect any issues with the security, availability and integrity of the infrastructure, software, and data. Alerts and logs are monitored with incident management processes defined for handling and resolving adverse events.

Clear21's critical infrastructure and data are hosted by Amazon Web Services (AWS) with multiple availability zones to provide failover capability in the event of an outage of one of the data centers. Redundancy, disaster recovery in continuity considerations is built into the system design of Amazon Web Services (AWS) to support Clear21's availability objectives. These are supported by the system monitoring, incident management processes and defined recovery and continuity plans.

Change Control

Clear21 operates a defined process for software development with supporting policies and procedures. Change requests and requirements are logged and prioritized for development. Changes include those related to functionality improvements, bug fixes, security and reliability-related enhancements, and other updates to the iBodyshop, RepairConnection, Clear21 Assessing software to support Clear21's System and objectives.

Separate environments are used to support development and testing activities in isolation from the production environment. GitHub version control software is used for the code repository that tracks all changes to the iBodyshop, RepairConnection, Clear21 Assessing software, including managing versions and roll-back capability in the event of a failed change release. A continuous integration / continuous deployment (CI/CD) pipeline is configured using TeamCity to enforce key process steps and checks prior to new versions of the code base being deployed into the production environment. Changes to the infrastructure configurations and settings are managed as code, subject to the same process steps and checks prior to impacting the production environment.

Data Governance

Clear21 uses data to support the System objectives and services. An approach to effective data governance has been established to understand and communicate the data that's used in the System, the objectives and requirements of that data, and the security, availability, and integrity commitments of Clear21.

Established processes, policies, procedures define the operational requirements for data governance, including how data is classified, handled, and used by the System in supporting the objectives and services.

Boundaries of the System

The scope of this report includes the Software as a Service System performed in the Sydney, Australia facilities.

This report does not include the cloud hosting services provided by AWS for the Sydney, Australia facilities.

Changes to the System 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.

Incidents in the Last 12 Months

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

Criteria Not Applicable to the System

All Common / Security and Confidentiality criteria were applicable to the Clear21's Software as a Service System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS for the Sydney, Australia facilities.

Subservice Description of Services

AWS provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world. With data center locations in the U.S., Europe, Brazil, Singapore, Japan, and Australia.

Complementary Subservice Organization Controls

Clear21's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Clear21's services to be solely achieved by Clear21 control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Clear21.

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

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		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.
		Physical access points to server locations are recorded by closed circuit television camera ('CCTV'). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply ('UPS') units provide backup power in the event of an electrical failure in Amazon-owned data centers.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.

Clear21 management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Clear21 performs monitoring of the subservice organization controls, including the following procedures:

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

COMPLEMENTARY USER ENTITY CONTROLS

Clear21'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 Trust Services Criteria related to Clear21's services to be solely achieved by Clear21 control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Clear21's.

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

1. User entities are responsible for understanding and complying with their contractual obligations to Clear21.
2. User entities are responsible for notifying Clear21 of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Clear21 services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize CLEAR21 services.
6. User entities are responsible for providing Clear21 with a list of approvers for security and system configuration changes for data transmission.

7. User entities are responsible for immediately notifying Clear21 of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.