Clear21

SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT ON MANAGEMENT'S DESCRIPTION OF ITS

Software as a Service System

Relevant to: Trust Services Criteria for Security and Confidentiality

For the period 1 December 2024 to 30 November 2025

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors' Report

To the Management of Clear21 Pty Ltd ('Clear21')

Scope

We have examined Clear 21 assertion titled "Assertion of Clear21" (assertion) that the controls within Clear21's Software as a Service System (system) were effective throughout the period 1 December 2024 to 30 November 2025, to provide reasonable assurance that Clear 21'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 SP section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022*) in AIPCA, *Trust Services Criteria.*

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 provided the accompanying 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 service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance the services 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the 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 were effective throughout the period 1 December 2024 to 30 November 2025, to provide reasonable assurance that Clear21's services commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Sensiba LLP

San Jose, California
24 February 2026

2. Assertion of Clear21 Management

We are responsible for designing, implementing, operating and maintaining effective controls within Clear21 Pty Ltd's (Clear21) Software as a Service System throughout the period 1 December 2024 to 30 November 2025 to provide reasonable assurance that Clear21's service commitments and system requirements relevant to Security and Confidentiality were achieved. Our description of the boundaries of the system is presented in the section of this report titled "Description of Clear21's Software as a Service System" (description) 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 1 December 2024 to 30 November 2025, 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 (With Revised Points of Focus — 2022) in AICPA, 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 the accompanying system description. 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 1 December 2024 to 30 November 2025, to provide reasonable assurance that Clear21's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by Clear21 Management

24 February 2026

3. Description of Clear21's Software as a Service System

Company Background

Clear21 Pty Ltd ('Clear21') is a SOC 2 compliant software company founded in 1996 with the objective of streamlining business processes via user-friendly, reliable, and cost-effective Software as a Service ('SaaS') solutions. It strives to achieve measurable and sustainable improvements for the business success and personal satisfaction of Clear21 customers.

Industries served by Clear21 include automotive smash repair, parts pricing and motor vehicle assessing services.

Services Provided

Clear21 supports customers across Australia, New Zealand and United Kingdom. Clear21's Software as a Service System (the 'System') comprises of three different products (the 'Products'):

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

- Calculating estimations.
- 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.

Repair Connection
Provides a parts marketplace where suppliers can perform activities from quotes to supplying parts to repairers.

Clear21 Assessing
A product allowing 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 Software as a Service 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 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

Clear21 utilizes industry-leading cloud service providers to ensure data integrity and availability.

People
Clear21's personnel 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.
- Project Management: Responsible for enterprise delivery of programs and projects to support the objectives.
- 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.
- Information Security: Responsible for managing information security controls, policies, and processes.
- 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, email, contact details.
- Business information: proprietary data of business activities and property.

Processes, Policies and Procedures
Processes, policies, and procedures are established that set the standards and requirements of the System. All personnel are expected to comply with Clear21's policies and procedures that define how the System should be managed. The documented policies and procedures are shared with all Clear21's employees and can be referred to as needed.

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

Logical Access
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. Microsoft Entra ID authentication software is used for identity management and single sign-on. Access management processes are followed to ensure new and modified access is approved, terminated users access is removed, and access rights are annually 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, continuous 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. Intune mobile device management software is used to monitor, systematically enforce device requirements, and provide remote management capabilities for the workstations.

System Operations
Backup and restoration procedures for the System are defined and followed. The System is monitored through a combination of automated and manual processes to prevent and detect any issues with 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 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 are built into the system design of 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 Products 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 Products, 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 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.

Control Environment
Integrity and Ethical Values

The effectiveness of controls is dependent on the integrity and ethical values of the people who implement, manage, and monitor them. Integrity and ethical values are important foundations of Clear21's control environment, affecting the design, implementation, and monitoring of the controls. Integrity and ethical behavior are supported by Clear21's culture, governance, hiring and onboarding practices, ethical and behavioral standards, the way those are communicated, and how they are reinforced in practice. 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.

Commitment to Competence

Clear21's competence of employees includes the knowledge and skills necessary to accomplish employees' roles and responsibilities, in support of Clear21's objectives and commitments.

Management's commitment to competence includes careful consideration of the competence levels required for each role, the requisite skills, knowledge, and experience, and the actual performance of individuals, teams and the company as a whole.

Management's Philosophy and Operating Style

Clear21's management philosophy and operating style is a purpose-driven, risk-based approach to pursuing the company objectives and satisfying Clear21's commitments. Risk taking is an essential part of pursuing the objectives. A formal approach is taken to understanding those risks and being deliberate about which risks are acceptable, and where risk mitigation actions are required.

Organizational Structure and Assignment of Authority and Responsibility

Clear21's organizational structure provides the framework within which its activities for achieving the objectives are planned, executed, managed, and monitored. An organizational structure has been developed to suit Clear21's needs and is revised over time as the company grows and requirements change.

Roles and responsibilities are further established and communicated through documented policies, and job descriptions, as part of individual performance review processes, reviewing and communicating team and functional performance, and the various operational team and governance meetings.

Human Resource Policies and Practices

Clear21's employees are the foundation for achieving the objectives and commitments. Clear21's hiring, onboarding and human resource practices are designed to attract, develop, and retain high-quality employees. That includes training and development, performance evaluations, compensation, and promotions, providing personal support and perks for individuals, recognizing team and company success, and building a culture of alignment to a shared purpose and vision. It also includes disciplinary processes and business planning to avoid single-person dependencies to ensure the objectives and commitments are not reliant on individuals.

Risk Assessment Process

Clear21's risk assessment process identifies and manages risks that threaten achievement of the objectives and commitments. This includes risks that may affect the security, reliability or integrity of the services provided to user organizations and other interested stakeholders.

A formal process is followed to identify, assess, treat, and monitor the risks to ensure the risks are aligned to the risk appetite and objectives of Clear21, and mitigated or avoided where appropriate. Risks identified in this process include:

- Operational risk – changes in the environment, staff, or management personnel, reliance on third parties, and threats to security, reliability, and integrity of Clear21's operations.
- Strategic risk – new technologies, changing business models, and shifts within the industry.
- Compliance risk – legal and regulatory obligations and changes.
- Financial risk – the sustainability of Clear21 and resources supporting the objectives.

These risks are identified by Clear21 management, employees, and third-party stakeholders, and updated in the risk register as a single source of monitoring the risks. The formal risk assessments ensure the ongoing commitment of management, and support completeness and an evolving view of the risk landscape in Clear21's context.

Integration with Risk Assessment

Established internal controls include Clear21's policies, procedures, automated system functions and manual activities. The controls are designed and implemented to address the identified risks, and to meet the obligations and criteria set by laws, regulations, customer commitments and other compliance obligations. The controls follow a continual improvement methodology in consideration of the costs and benefits of such control improvements and recognizing the changing landscape and requirement of those controls as Clear21 grows, and the associated risks change.

Information and Communications Systems

Information and communication are a core part of Clear21'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 Clear21's operations effectively. The information and communication systems consider the internal control requirements, operating requirements, and the needs of interested parties including employees, customers, third-party vendors, regulators, and shareholders.

The information and communication systems include central tracking systems that support Clear21's established processes, as well as various meetings, and documented policies, procedures, and organizational knowledge.

Monitoring Controls

Management monitors the controls to ensure that they are operating as intended and that controls are modified and continually improved over time. Leadership, culture, and communication of the controls are important enablers to the effectiveness of the controls in practice. This ensures buy-in amongst the employees and empowers Clear21's team and individuals to prioritize the performance and continual improvement of the controls. Evaluations are performed during the course of business, in management reviews, and by independent auditors to assess the design and operating effectiveness of the controls. Deficiencies that are identified are communicated to responsible control owners to agree remediation actions or re-

enforce the control requirements and importance. Corrective actions are tracked with agreed timelines and ownership for remediation with ownership of management and the board, for ensuring appropriate actions are completed in a timely manner.

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 examination 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 examination period.

Criteria Not Applicable to the System

All Security and Confidentiality Trust Services Criteria were applicable to Clear21's Software as a Service System.

Subservice Organizations
This report does not include the cloud hosting services provided by AWS.

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 Agreed 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 Agreed Criteria described within this report are met.

Subservice Organization – AWS		
Category	Criteria	Control
Security	CC6.1-CC6.8	Logical access measures are established and followed to ensure access to systems and data is restricted to authorized personnel with technical safeguards and ongoing assessments to reduce the risk of system and data breaches.
Security	CC6.4	Policies and procedures are established and followed to restrict physical access to data center facilities, backup media, and other system components, including firewalls, routers, and servers.
Security	CC7.1-CC7.5	Incident management and response policies and procedures are established and followed to identify, analyze, classify, respond to and resolve adverse events.
Security	CC8.1	Formal processes are established and followed to ensure system changes are documented, tracked, prioritized, developed, tested and approved prior to deployment into production.

Clear21 management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Agreed Criteria through written contracts and published terms of service. In addition, Clear21 performs monitoring of the subservice organization controls by reviewing attestation reports and monitoring the performance of the subservice organization controls.

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 Agreed 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 Agreed 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.

User entities are responsible for:

- Understanding and complying with Clear21's terms of service.
- Notifying Clear21 of changes made to technical or administrative contact information.
- Administering their users' access rights including approval, removal, and periodic review to ensure access is appropriate.
- Ensuring multi-factor authentication is applied by personnel, if required.
- Performing any required risk assessments and approvals when using pre-built integrations available with Clear21's services.
- Performing any required risk assessments and approvals for using Clear21's open application programming interface (API), and notifying Clear21 of any identified vulnerabilities, security breaches or system failures when using the APIs.
- Ensuring the supervision, management, and control of the use of Clear21's services by their personnel.
- Developing their own disaster recovery and business continuity plans that address the inability to access or utilize Clear21 services for any critical reliance on these services.
- Immediately notifying Clear21 of any actual or suspected information security breaches or system failures.