# Clear21 Pty Ltd
# SOC 3 for Service Organisations Report

**1 December 2022 to 30 November 2023**

assurancelab

# CONTENTS

# SECTION I –
# ASSERTION OF CLEAR21 PTY LTD MANAGEMENT

## ASSERTION OF CLEAR21 PTY LTD MANAGEMENT

9 February 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within Clear21 Pty Ltd's ('Clear21') Software as a Service System (the 'System') throughout the period 1 December 2022 to 30 November 2023, 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 ('Agreed 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 in 'Clear21 Pty Ltd's Description of its System' (the '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 2022 to 30 November 2023, to provide reasonable assurance that Clear21's service commitments and system requirements were achieved based on the Agreed Criteria. Clear21's objectives for the system in applying the Agreed Criteria are embodied in its service commitments and system requirements relevant to the Agreed Criteria. The principal service commitments and system requirements related to the Agreed Criteria are presented in 'Clear21's Pty Ltd's Description of its System'.

Clear21 uses Amazon Web Services ('AWS' or 'subservice organisation') to provide cloud hosting services. The Description indicates that complementary subservice organisation 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 Agreed Criteria. The Description presents Clear21's controls, the Agreed Criteria, and the types of complementary subservice organisation controls assumed in the design of Clear21's controls. The Description does not disclose the actual controls at the subservice organisation.

The Description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at Clear21, to achieve Clear21's service commitments and system requirements based on the Agreed Criteria. The Description presents Clear21's controls, the Agreed 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 organisation 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 2022 to 30 November 2023, to provide reasonable assurance that Clear21's service commitments and system requirements were achieved based on the Agreed Criteria.

Glendon Smith
Chief Operating Officer
Clear21 Pty Ltd

# SECTION II –
# INDEPENDENT SERVICE AUDITOR'S REPORT

**INDEPENDENT SERVICE AUDITOR'S REPORT**

To: Clear21 Pty Ltd

**Scope**

We have examined Clear21 Pty Ltd's ('Clear21') accompanying description of its Software as a Service System (the 'Description') which has been prepared for the purposes of the independent assurance report.

Clear21 prepared the Description based on the following description criteria ('Description Criteria'):

- SOC 2: the criteria for a description of a service organisation's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) with regards to the Description.

The Description is intended to provide report users with information about Clear21's Software as a Service System (the 'System') that may be useful when assessing the risks arising from interactions with Clear21's system. This includes the controls that Clear21 has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the following agreed criteria ('Agreed Criteria'):

- SOC 2: the trust services criteria relevant to Common Criteria/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 (AICPA, Trust Services Criteria).

Clear21 uses Amazon Web Services ('AWS' or 'subservice organisation') to provide cloud hosting services. The Description indicates that complementary subservice organisation 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 Agreed Criteria. The complementary subservice organisation controls have been reviewed by Clear21 management. The Description does not disclose the actual controls at the subservice organisation. Our examination did not include the services provided by the subservice organisation, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organisation controls.

The Description includes complementary user entity controls that are necessary, along with controls at Clear21, to achieve Clear21's service commitments and system requirements based on the Agreed Criteria. The Description presents Clear21's controls, the Agreed Criteria and the complementary user entity controls assumed in the design of Clear21's controls. The complementary user entity controls have not been assessed by our examination and remain the responsibility of those related entities to complete their own review.

**Service Organisation'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 titled "Assertion of Clear21 Pty Ltd Management" (the 'Assertion') about the Description and the suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the Agreed Criteria. Clear21 is also responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion; providing the services covered by the Description; selecting the applicable Agreed Criteria and stating the related controls in the Description; and identifying the risks that threaten the achievement of the Clear21's service commitments and system requirements.

**Service Auditor's Responsibilities**

Our responsibility is to express an opinion on the Description and on the suitability of the design and operating effectiveness of controls stated in the Description based on our examination. Our examination was conducted in accordance with AT-C 105 and AT-C 205 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects:

- The Description is presented in accordance with the Description Criteria.
- The controls stated in the Description were suitably designed.
- The controls stated in the Description were operating effectively throughout the period to provide reasonable assurance that Clear21's service commitments and system requirements were achieved based on the Agreed Criteria.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the Description of Clear21's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the System and Clear21'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.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the Description Criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that Clear21 achieved its service commitments and system requirements based on the Agreed Criteria.

- Testing the operating effectiveness of controls stated in the Description to provide reasonable assurance that Clear21 achieved its service commitments and system requirements based on the Agreed Criteria.
- Evaluating the overall presentation of the Description.

**Inherent Limitations**

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the System that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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 effective throughout the period 1 December 2022 to 30 November 2023, to provide reasonable assurance that Clear21's service commitments and system requirements were achieved based on the Agreed Criteria is fairly stated, in all material respects.

Erika Villanueva

Erika Villanueva, CA, CPA
AssuranceLab Pty Ltd
Sydney, Australia
9 February 2024

# SECTION III –
# CLEAR21 PTY LTD'S DESCRIPTION OF ITS SYSTEM

# OVERVIEW OF OPERATIONS

## 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.

## Description of Services Provided

Clear21 supports customers across Australia and New Zealand. 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 authorise insurance claims.

## Principal Service Commitments and System Requirements

Clear21 has established processes, policies, and procedures to meet its objectives related to its iBodyshop, Repair Connection and Clear21 Assessing Products. 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 Products. The operational requirements are communicated in Clear21's processes,

policies and procedures, system design documentation, and customer agreements. This includes policies around how the Products are designed and developed, how the Products operate, how the system components are managed, and how employees are hired, developed, and managed to support the Products.

## *Components of the System*

### Infrastructure

Clear21's primary infrastructure used to provide iBodyshop, Repair Connection and Clear21 Assessing (the 'Products') includes the cloud hosted networking, compute, and database components of Amazon Web Services ('AWS').

| System | Type | Description |
|---|---|---|
| **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. |
| **AWS ElastiCache** | Cloud Compute | Serverless, Redis-compatible caching service. |
| **AWS Simple Storage Service (S3)** | Data Storage | Object, file, and block storage. |
| **Amazon Aurora PostgreSQL** | Data Storage | Open-source relational database management system emphasizing extensibility and SQL compliance. |
| **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 Route 53** | Networking | Highly available and scalable cloud domain name system (DNS) service. |
| **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 Products.

| Software | Purpose |
|---|---|
| **iBodyshop, Repair Connection, Clear21 Assessing** | The Software as a Service products 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. |
| **Microsoft Entra ID** | Authentication software used to identify and authenticate users for access control to the systems. |
| **GitHub** | Source code repository used to manage the software code and version control. |
| **TeamCity** | Continuous integration / continuous delivery 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. |
| **Microsoft Intune** | Mobile device management software used to track and manage security policies on endpoint devices. |
| **ESET** | Antivirus software used to protect endpoint devices from malware. |
| **Sophos** | Security management and operations software used to manage the network, including firewall, antivirus, and endpoint device management. |
| **Datadog** | System monitoring software used to log events and raise alerts to support system security and availability. Security and compliance software used to monitor and manage the security, risk, and control activities to support compliance. |
| **Dependabot** | Vulnerability scanning software to identify, log and resolve technical vulnerabilities. |
| **Jira** | Ticketing software used to log events and requirements to support the internal controls. |

| Software | Purpose |
|---|---|
| **ELMO** | Human resources information system used to manage employee processes like onboarding, offboarding and performance. |
| **Zendesk** | Customer service and customer relationship management software. |
| **Slack** | Communication software used to facilitate real-time communication in the form of text chat or voice chat within the company and with external parties. |
| **Confluence** | Content collaboration and management workplace built for teams. |
| **Office 365** | Microsoft's suite of enterprise productivity, collaboration, and communication tools. |

### People

Clear21 has 55 people that are organised 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.
- 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 and contact details.
- User activity: user activity within the software.
- Financial account information: account balances and transactions.

## *Processes, Policies and Procedures*

Processes, policies, and procedures are established that set the standards and requirements of the Clear21 Products. All personnel are expected to comply with Clear21's policies and procedures that

define how the Products 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 Amazon Web Services ('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 authorised 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 multi-factor authentication. 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 authorised manner.

Automated and manual security practices are used to protect the perimeter security and network to prevent unauthorised 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 unauthorised 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. Microsoft Intune, Sophos and ESET 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 are defined and followed. The Products are 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 centres. Redundancy, disaster recovery and 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 prioritised 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 its Products, objectives, and services. An approach to effective data governance has been established to understand and communicate the data that's used in the Products, the objectives and requirements of that data, and the commitments of Clear21.

Established processes, policies and 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 iBodyshop, Repair Connection, Clear21 Assessing Software as a Service System. This report does not include the cloud hosting services provided by Amazon Web Services ('AWS').

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

## *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 behaviour are supported by Clear21's culture, governance, hiring and onboarding practices, ethical and behavioural 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 behavioural 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.

### Organisational Structure and Assignment of Authority and Responsibility

Clear21's organisational structure provides the framework within which its activities for achieving the objectives are planned, executed, managed, and monitored. An organisational 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, recognising 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*

### Risk Assessments

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 organisations 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 – legal and regulatory obligations and changes.
- Financial – 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 recognising 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 organisational 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 prioritise 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*

### SOC 2

All Common Criteria/Security and Confidentiality Trust Services Criteria were applicable to Clear21's Products.

# COMPLEMENTARY SUBSERVICE ORGANISATION CONTROLS

This report does not include the cloud hosting services provided by Amazon Web Services ('AWS').

## 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 centre locations in the U.S., Europe, Brazil, Singapore, Japan, and Australia.

## Complementary Subservice Organisation Controls

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

The following subservice organisation controls should be implemented by AWS to provide additional assurance that the Agreed Criteria described within this report are met.

| Subservice Organisation – Amazon Web Services | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| Common Criteria/ Security | CC6.1-CC6.8 | Logical access measures are established and followed to ensure access to systems and data is restricted to authorised personnel with technical safeguards and ongoing assessments to reduce the risk of system and data breaches. |
| | CC6.4 | Physical access to data centres is approved by an authorised individual. |
| | | Physical access is revoked within 24 hours of the employee or vendor record being deactivated. |
| | | Physical access to data centres 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. |

| Subservice Organisation – Amazon Web Services | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| | CC7.1-CC7.5 | Incident management and response policies and procedures are established and followed to identify, analyse, classify, respond to, and resolve adverse events. |
| | 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 organisation, 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 organisation controls by reviewing attestation reports and monitoring the performance of the subservice organisation 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 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 utilise Clear21 services for any critical reliance on these services.
- Immediately notifying Clear21 of any actual or suspected information security breaches or system failures.

assurancelab