ScreenCloud Inc.'s SOC 3 for Service Organizations Report

1 June 2023 to 31 May 2024

Contents

Section I

ASSERTION OF SCREENCLOUD INC. MANAGEMENT

ASSERTION OF SCREENCLOUD INC. MANAGEMENT

July 4, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within ScreenCloud Inc. (‘ScreenCloud) Software as a Service System (the ‘System’) throughout the period 1 June 2023 to 31 May 2024 to provide reasonable assurance that ScreenCloud’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, 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 ‘ScreenCloud’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 June 2023 to 31 May 2024 to provide reasonable assurance that ScreenCloud’s service commitments and system requirements were achieved based on the Agreed Criteria. ScreenCloud’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 ‘ScreenCloud’s Description of its System.

ScreenCloud use Amazon Web Services ('AWS') and Microsoft Azure ('Azure') (collectively known as the 'subservice organizations') to provide cloud hosting services. The Description indicates that complementary subservice organizations controls that are suitably designed and operating effectively are necessary, along with controls at ScreenCloud, to achieve ScreenCloud’s service commitments and system requirements based on the Agreed Criteria. The Description presents ScreenCloud’s controls, the Agreed Criteria, and the types of complementary subservice organization controls assumed in the design of ScreenCloud’s controls. The Description does not disclose the actual controls at the subservice organizations.

The Description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at ScreenCloud, to achieve ScreenCloud’s service commitments and system requirements based on the Agreed Criteria. The Description presents ScreenCloud’s controls, the Agreed Criteria, and the complementary user entity controls assumed in the design of ScreenCloud’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.

Luke Hubbard

Luke Hubbard
Chief Technology Officer
ScreenCloud Inc.

Section II

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: ScreenCloud Inc.

Scope

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

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

- SOC 2: the criteria for a description of a service organization'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 the ScreenCloud Software as a Service System (the 'System') that may be useful when assessing the risks arising from interactions with ScreenCloud's system. This includes the controls that ScreenCloud 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, Availability, 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).

ScreenCloud use Amazon Web Services ('AWS') and Microsoft Azure ('Azure') (collectively known as the 'subservice organizations') to provide cloud hosting services. The Description indicates that complementary subservice organizations controls that are suitably designed and operating effectively are necessary, along with controls at ScreenCloud, to achieve ScreenCloud's service commitments and system requirements based on the Agreed Criteria. The complementary subservice organizations controls have been reviewed by ScreenCloud management. The Description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organizations controls.

The Description includes complementary user entity controls that are necessary, along with controls at ScreenCloud, to achieve ScreenCloud's service commitments and system requirements based on the Agreed Criteria. The Description presents ScreenCloud's controls, the Agreed Criteria, and the complementary user entity controls assumed in the design of ScreenCloud'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 Organization's Responsibilities

ScreenCloud 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 ScreenCloud's service commitments and system requirements were achieved. ScreenCloud has provided the accompanying assertion titled "Assertion of ScreenCloud 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. ScreenCloud 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 ScreenCloud'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 ScreenCloud'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 ScreenCloud's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and ScreenCloud'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 ScreenCloud 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 ScreenCloud 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.

Because of the inherent limitations of any internal control structure it is possible that, even if the controls are suitably designed and operating effectively, the control objectives may not be achieved and so fraud, error, or non-compliance with laws and regulations may occur and not be detected.

An assurance engagement on operating effectiveness of controls is not designed to detect all instances of controls operating ineffectively as it is not performed continuously throughout the period and the tests performed are on a sample basis. Any projection of the outcome of the evaluation of controls to future periods is subject to the risk that the controls may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

Opinion

In our opinion, management's assertion that the controls within ScreenCloud's Software as a Service System were effective throughout the period 1 June 2023 to 31 May 2024, to provide reasonable assurance that ScreenCloud's service commitments and system requirements were achieved based on the Agreed Criteria is fairly stated, in all material respects.

AssuranceLab CPAs LLC

AssuranceLab CPAs LLC
Austin, Texas
United States
July 4, 2024

Section III

SCREENCLOUD INC.'S DESCRIPTION OF ITS SYSTEM

OVERVIEW OF OPERATIONS

Company Background

ScreenCloud Inc. ('ScreenCloud') was founded in 2015, headquartered in London, UK with additional offices in Los Angeles, Charlotte, Belfast, and Bangkok. ScreenCloud is a cloud-based content management software for digital signage networks of any size. It provides a solution that helps businesses connect their workplaces with employee-facing 'screens that communicate'; with a focus on reaching and engaging deskless or frontline workers. ScreenCloud's solution also caters for the use cases of student- and customer-facing screens.

ScreenCloud serves customers in key sectors such as manufacturing, retail, hospitality and retail, events, franchise management, education, fitness and places of worship.

Description of Services Provided

With ScreenCloud, companies can:

- Display and control meaningful content on one, or thousands of digital screens anywhere in the world.
- Creatively elevate information. An integrated digital screen experience increases visibility of key messages across entire organizations and key audiences.
- Increase employee and customer attention by displaying important updates, campaigns or product information in a visual and engaging format.
- Digitise traditional communication approaches by providing a modern cloud-based platform that can control an organization's digital signage content flow and screens remotely.

ScreenCloud is hardware and operating-system agnostic – the software runs on almost any media player which allows customers to turn any screen or device they already have into a digital screen. The focus is on putting the power of the software solution in the hands of communication experts and content creators versus the IT department, through supporting consumer-grade hardware and providing a simple self-serve UX.

ScreenCloud also specialises in customizable content curation with an eco-system of 70+ apps and integrations, including Microsoft 365, Slack, Instagram, and CNN for customers to curate effective screen content.

Principal Service Commitments and System Requirements

ScreenCloud 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 ScreenCloud as well as commitments that ScreenCloud makes to user entities, the requirements of laws and regulations that apply to ScreenCloud's activities, and the operational requirements that ScreenCloud 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 ScreenCloud'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

ScreenCloud's primary infrastructure used to provide the System includes the cloud hosted networking, compute and database components of Amazon Web Services ('AWS') and Microsoft Azure ('Azure').

System	Type	Description
Azure Kubernetes Service (AKS)	Cloud Compute	Deploy and scale containers on managed Kubernetes
Azure Database for Postgres	Data Storage	Storage of client data.
Azure Blob Storage	Data Storage	Storage of client documents.
Azure Load Balancer	Networking	Distributes incoming traffic among virtual machines.
Azure Firewall	Network Firewall	A cloud-native network firewall security service that provides threat protection for cloud workloads running in Azure.
Azure Web Application Firewall	Web Application Firewall	A cloud-native service that protects web apps from common web-hacking techniques such as SQL injection and security vulnerabilities such as cross-site scripting.
Azure Key Vault	Encryption	A cloud service to securely store keys, passwords, certificates, and other secrets.
AWS Elastic Container Service (ECS)	Cloud Compute	Secure, reliable, and scalable service to run containers.
AWS Lambda	Cloud Compute	Serverless, event-driven compute service.
AWS RDS	Data Storage	Relational database service.
AWS Simple Storage Service (S3)	Data Storage	Object, file, and block storage.
AWS Firewall Manager	Firewall Manager	Security management service to centrally configure and manage firewall rules across accounts and applications in AWS Organizations.
AWS Web Application Firewall	Web Application Firewall	Protects web applications or APIs against common web exploits and bots that may affect availability,

System	Type	Description
		compromise security, or consume excessive resources.
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.
Cloudflare	Network Services	Image and video optimization for cross-platform screen delivery via CDN.

Software

Primary software is used to support ScreenCloud's system.

Software	Purpose
Studio	The Software as a Service System provided to ScreenCloud 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.
Google SSO	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.
GitHub Actions	Continuous integration / continuous delivery software used to manage the pipeline of change release testing and deployment.

Software	Purpose
LastPass	Enterprise password manager used to store authentication secrets and strengthen password security.
JAMF	Mobile device management software used to track and manage security policies on endpoint devices.
ESET	Anti-virus software used to protect endpoint devices from malware.
DataDog	System monitoring software used to log events and raise alerts to support system security and availability.
Aikido	Vulnerability scanning software to identify, log and resolve technical vulnerabilities.
GitHub Issues	Ticketing software used to log events and requirements to support the internal controls.
Zluri	SaaS management information system used to monitor and control ScreenCloud's SaaS stack, monitor shadow IT, optimize costs, and manage employee processes like onboarding, offboarding and provisioning for company systems.
Google Workspace	Google's suite of enterprise productivity, collaboration, and communication tools.
Drata	Security and compliance software used to monitor and manage the security, risk, and control activities to support compliance.

People

ScreenCloud has approximately 122 people that are organized into the following functional areas:

- **Senior Leadership**: Includes the CEO, CFO, CTO, VP Customer Success, VP of Sales and VP of Marketing. They are responsible for the overall governance of ScreenCloud, formulating its strategy and structure, overseeing company-wide activities, and protection of the company's assets and reputation.
- **Business support**: The Team consists of Cyber Security & company administrative support staff, such as Finance and People & Culture. These people provide support in the day to day running of the company ensuring companywide objectives are met.
- **Engineering**: The Engineering Team is led by the CTO, who provides strategic direction for the engineering department, and line management to three Directors of Engineering. They are responsible for the development of the software as well as making improvements and enhancements to it as per the business needs. Main responsibilities include:
    - Building, testing and deploying code and feature changes
    - Maintaining service availability and configuration management
    - Providing monitoring, scanning and penetration testing

- Maintaining business continuity disaster recovery capabilities
- Ensuring a simple and powerful user interface of the product

- **Product:** Responsible for understanding and validating market opportunities as expressed through customer requirements, defining feature requests and bringing the product vision to life.
- **Marketing**: Responsible for defining and managing the brand, building pipeline, enabling sales, monitoring and managing social media, producing internal and external communications, educating customers through content and producing marketing and promotional materials.
- **Professional Services**: Provides ScreenCloud's enterprise clients bespoke innovative services such as onboarding and training, project management, content strategy, design services, bespoke application development and account auditing and optimizations.
- **Customer Support**: ScreenCloud has a growing customer support team based in all of our hubs, making sure 24/5 support to customers is provided in a timely and efficient manner. The main goal of the Team is to answer, solve, track and escalate all pre-sales and post-sales questions or problems.
- **Customer Success**: Responsible for the post-sale relationships with ScreenCloud's existing customers. Focusing on customer adoption, customer advocacy, churn reduction, customer training and proving ROI.
- **Enterprise Account Management**: Commercially focused department responsible for developing new business and expansion opportunities from existing customers.

Data

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

- The data collected and processed by ScreenCloud includes the following types:
- Organizational account subscription data
- User account data
- App configuration data
- Screens content configuration data
- User uploaded content
- System files
- Error logs

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 ScreenCloud's policies and procedures that define how the System should be managed. The documented policies and procedures are shared with all ScreenCloud's employees and can be referred to as needed.

Compliance Management Platform

ScreenCloud uses compliance automation software, Drata, to support the design, implementation, operation, monitoring, and documentation of internal controls. Drata leverages APIs to centralize the monitoring of ScreenCloud's information assets across their infrastructure provider, identity manager, code repository, and endpoint devices. These APIs in combination with compliance automation functions in Drata supports the continuous monitoring of control activities for ScreenCloud's people, devices, policies, procedures and plans, risk assessments, third-party vendor assessments, system monitoring and the security configurations of these critical systems.

Using Drata does not reduce management's responsibility for designing, implementing, and operating an effective system of internal control. ScreenCloud evaluates the accuracy and completeness of the information stored in Drata and conducts annual vendor risk assessments.

Logical Access

ScreenCloud'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. Google SSO 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 reviewed annually and adjusted when no longer required. Additional information security policies and procedures require ScreenCloud 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, monthly testing for and remediation of technical vulnerabilities and applying network controls like firewalls and event monitoring to prevent and detect unauthorized activity.

ScreenCloud 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. JAMF mobile device management software, the Drata agent, and ESET Protect Anti-Virus 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.

ScreenCloud's critical infrastructure and data are hosted by AWS and Azure 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 and Azure to support ScreenCloud's availability objectives. These are supported by the system monitoring, incident management processes and defined recovery and continuity plans.

Change Control

ScreenCloud 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 Studio software to support ScreenCloud'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 Studio 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 GitHub Actions to enforce key process steps and checks prior to new versions of the code base being deployed into the production environment.

Data Governance

ScreenCloud 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 ScreenCloud.

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 (the 'System'). This report does not include the cloud hosting services provided by AWS and Azure.

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 Common Criteria/Security, Availability, and Confidentiality Trust Services Criteria were applicable to ScreenCloud's Software as a Service System.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

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

Subservice Description of Services

AWS

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.

Azure

Microsoft Azure, commonly referred to as Azure, is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers.

Complementary Subservice Organization Controls

ScreenCloud'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 ScreenCloud's services to be solely achieved by ScreenCloud control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of ScreenCloud.

AWS

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**
Common Criteria/ 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.
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.

Subservice Organization – AWS		
Category	**Criteria**	**Control**
Common Criteria/ 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.
Common Criteria/ 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.
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.
		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.

Azure

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

Subservice Organization – Azure		
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 authorized personnel with technical safeguards and ongoing assessments to reduce the risk of system and data breaches.
Common Criteria/ Security	CC6.4	Procedures have been established to restrict physical access to the data center to authorized employees, vendors, contractors, and visitors.

Subservice Organization – Azure		
Category	**Criteria**	**Control**
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		Security verification and check-in are required for personnel requiring temporary access to the interior data center facility including tour groups or visitors.
		The data center facility is monitored 24x7 by security personnel.
		Physical access to the data center is reviewed quarterly and verified by the data center management team.
Common Criteria/ 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.
Common Criteria/ 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.
Availability	A1.2	Azure has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements.
		The BCP team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly.
		Backups of key Azure service components and secrets are performed regularly and stored in fault-tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.
		Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.
		Customer data is automatically replicated within Azure to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups.
		Azure services are configured to automatically restore customer services upon detection of hardware and system failures.
		Data center Management team maintains and tests data center-managed environmental equipment within the facility according to documented policy and maintenance procedures.

Subservice Organization – Azure		
Category	**Criteria**	**Control**
		Environmental controls have been implemented to protect systems inside data center facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.

ScreenCloud management, along with the subservice organizations, 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, ScreenCloud performs monitoring of the subservice organization controls by reviewing attestation reports and monitoring the performance of the subservice organization controls.

COMPLEMENTARY USER ENTITY CONTROLS

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

- User entities organizations are responsible for understanding and complying with their contractual obligations to ScreenCloud.
- User entities are responsible for notifying ScreenCloud of changes made to technical or administrative contact information.
- User entities are responsible for maintaining their own system(s) of record.
- User entities are responsible for ensuring the supervision, management, and control of the use of ScreenCloud's services by their personnel.
- User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilise ScreenCloud's services.
- User entities are responsible for ensuring that user IDs and passwords are assigned to only authorised individuals.
- User entities are responsible for ensuring that data submitted to ScreenCloud is complete, accurate, and timely.
- Standards and processes are in place for user entities to follow for security, confidentiality and industry guidelines.
- User entities are responsible for reporting identified security incidents to ScreenCloud.
- User entities are responsible for maintaining accurate and up to date contact information for ScreenCloud's use.
- User entities are responsible for maintaining accurate display records used with the ScreenCloud provided service.
- User entities are responsible for deploying local antivirus protection for owned devices used with the ScreenCloud provided service.
- User entities are responsible for reporting service failure to the ScreenCloud service support desk.
- User entities are responsible for ensuring the correct and legal use of data displayed on the ScreenCloud service.
- User entities are responsible for monitoring ScreenCloud Service Status pages for up-to-date service availability and defined maintenance periods @ https://status.screencloud.com/

Office Locations

AUSTRALIA
Level 3/11 York Street
Sydney NSW 2000

UNITED STATES
1400 Lavaca Street, Suite 700
Austin, Texas 78701

EMEA
Block 2 Charlemont Street, Charlemont Row
Saint Kevin’s, Dublin, D01 F6X6