A-LIGN

SnapComms, Inc.
an Everbridge Company

Type 2 SOC 3

2023

everbridge snapcomms

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

April 1, 2022 to March 31, 2023

Table of Contents

SECTION 1 ASSERTION OF SNAPCOMMS, INC. AN EVERBRIDGE COMPANY MANAGEMENT....... 1

SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT 3

SECTION 3 SNAPCOMMS, INC. AN EVERBRIDGE COMPANY'S DESCRIPTION OF ITS SNAPCOMMS PLATFORM THROUGHOUT THE PERIOD APRIL 1, 2022 TO MARCH 31, 2023.......... 7

OVERVIEW OF OPERATIONS 8
Company Background 8
Description of Services Provided 8
Principal Service Commitments and System Requirements 8
Components of the System 10
Boundaries of the System 15
Changes to the System in the Last 12 Months 15
Incidents in the Last 12 Months 15
Criteria Not Applicable to the System 15
Subservice Organizations 15
COMPLEMENTARY USER ENTITY CONTROLS 20

SECTION 1

ASSERTION OF SNAPCOMMS, INC. AN EVERBRIDGE COMPANY MANAGEMENT

ASSERTION OF SNAPCOMMS, INC. AN EVERBRIDGE COMPANY MANAGEMENT

May 18, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within SnapComms, Inc. an Everbridge Company's ('SnapComms' or 'the Company') SnapComms Platform throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that SnapComms' service commitments and system requirements were achieved based on the trust services criteria relevant to 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*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "SnapComms, Inc. an Everbridge Company's Description of Its SnapComms Platform throughout the period April 1, 2022 to March 31, 2023" 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 April 1, 2022 to March 31, 2023, to provide reasonable assurance that SnapComms' service commitments and system requirements were achieved based on the trust services criteria. SnapComms' 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 "SnapComms, Inc. an Everbridge Company's Description of Its SnapComms Platform throughout the period April 1, 2022 to March 31, 2023".

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

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

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

We assert that the controls within the system were effective throughout the period April 1, 2022 to March 31, 2023 to provide reasonable assurance that SnapComms' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of SnapComms' controls operated effectively throughout that period.

Karen Meohas

Karen Meohas
Senior Director of Global Compliance
SnapComms, Inc. an Everbridge Company

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To SnapComms, Inc. an Everbridge Company:

Scope

We have examined SnapComms' accompanying assertion titled "Assertion of SnapComms, Inc. an Everbridge Company Management" (assertion) that the controls within the SnapComms Platform were effective throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that SnapComms' service commitments and system requirements were achieved based on the trust services criteria relevant to 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*, in AICPA *Trust Services Criteria*.

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

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

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

Our examination included:

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

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

Independence and Ethical Responsibilities

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

Inherent Limitations

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

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

Opinion

In our opinion, management’s assertion that the controls within the SnapComms Platform were suitably designed and operating effectively throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that SnapComms’ service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of SnapComms’ controls operated effectively throughout that period.

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

Restricted Use

This report, is intended solely for the information and use of SnapComms, user entities of the SnapComms Platform during some or all of the period April 1, 2022 to March 31, 2023, business partners of SnapComms subject to risks arising from interactions with the SnapComms Platform, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements.

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

A-LIGN ASSURANCE

Tampa, Florida
May 18,2023

SECTION 3

SNAPCOMMS, INC. AN EVERBRIDGE COMPANY’S DESCRIPTION OF ITS SNAPCOMMS PLATFORM THROUGHOUT THE PERIOD APRIL 1, 2022 TO MARCH 31, 2023

OVERVIEW OF OPERATIONS

Company Background

SnapComms grew out of a small development company called 174E with a single customer, Vodafone New Zealand. Determined to help more organizations improve cut through for employee communications, the founders productized the offering and launched SnapComms in 2007. Within three years, SnapComms grew in the competitive sector of employee communication software and has enabled businesses across the world to send more than 1 billion messages to employees.

In August 2020, SnapComms was acquired by Everbridge Inc, a global software company that provides enterprise software applications across the critical events space. SnapComms serves different types of industries such as: Financial Services, telecommunications, Legal Services, Advertising, Manufacturing, Healthcare, Retail, Educational institutions, and Government agencies.

Description of Services Provided

SnapComms is a multi-channel, multidevice internal communications platform. Messages are created using the secure, cloud based SnapComms Content Manager and sent to employees who have the SnapComms App installed on their computer, tablet, or smartphone. These messages can be in the form of Desktop Alerts, Tickers, Surveys and Quizzes, Screensavers, Wallpapers and Lock Screens, or Newsletters.

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of SnapComms. Commitments are communicated in SnapComms' Master Service Agreement (MSA).

System requirements are specifications regarding how SnapComms should function to meet SnapComms principal commitments to user entities. System requirements are specified in SnapComms policies and procedures.

SnapComms' principal service commitments and system requirements related to the SnapComms Platform include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• SnapComms implements appropriate technical and organizational measures to protect client data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the data • SnapComms implements measures to remedy or mitigate the effects of a security incident and to keep the client informed of all developments of such an event	• Access controls for access to all systems and data • Risk assessments • Change management controls • Encryption standards

Trust Services Category	Service Commitments	System Requirements
Availability	- SnapComms will ensure 24/7/365 technical support availability - SnapComms will implement measures to remedy or mitigate the effects of an availability incident and to keep the client informed of all developments of such an event	- Monitoring controls - Backup and recovery standards - Disaster recovery plan
Confidentiality	- SnapComms will not disclose any confidential information to any person or entity other than the representatives of SnapComms who have a need to know such information in the course ofz the performance of their duties - Upon any termination of services, SnapComms will continue to maintain the confidentiality of the customer’s confidential information and, upon request and to the extent practicable, destroy all materials containing such confidential information - SnapComms will notify the customer if SnapComms becomes aware of a breach of confidentiality - SnapComms will protect the customer’s confidential information in the same manner that it protects its own confidential information, but in no event using less than reasonable care	- Data classification - Retention and destruction policy - Mutual Non-disclosure agreements (MNDAs) - Employee training - Employment agreements

Components of the System

Infrastructure

SnapComms utilizes Microsoft Azure (“Azure”) to provide the resources to host SnapComms’ infrastructure. SnapComms leverages the experience and resources of Azure to support the scalability, availability, and durability of the SnapComms Platform.

Primary infrastructure used to provide the SnapComms Platform includes the following:

Primary Infrastructure	
Production Service	**Business Function**
Azure SQL Database	Data storage
Azure Virtual Network	Networking and distributed denial-of-service (DDoS) protection
Azure App Service	Application hosting
Azure Functions	Task execution
Azure Service Bus	Queueing services
Azure Key Vault	Management of cryptographic keys
Azure DevOps	Code repository and continuous integration/continuous delivery (CI/CD) services
Azure Defender	Intrusion detection system (IDS)
Azure SQL Database	Data storage

Software

Primary software used to provide the SnapComms Platform includes the following:

Primary Software	
Production Application	**Business Function**
StackPath Content Delivery Network	Content delivery services
Jira	Bug and feature tracking
Zendesk	Help desk, ticketing system
Site24x7	Monitoring and alerting
Grafana	Monitoring and alerting
Sophos	Antivirus
DNS Made Easy	Domain Name System (DNS) services
Elastic	Application logging
Cisco VPN	Virtual Private Network (VPN)

People

SnapComms is comprised and supported by the following teams responsible for the delivery and management of the SnapComms Platform:

- Engineering: Responsible for the development, testing, deployment, and maintenance of new code for SnapComms
- Site Reliability Engineers (SRE): Responsible for managing access controls, monitoring the infrastructure, and maintaining the security of the production environment
- Product Management: Responsible for overseeing the product life cycle, including adding new product functionality
- Compliance and Information Security Team: Responsible for ensuring the integrity, availability, and confidentiality of customer data is protected at every stage of the product life cycle and across all Company processes
- Information Security Team: Supports SnapComms Platform by monitoring Internal and external security threats and maintaining security systems including malware and antivirus as required
- People and Culture Department: Defines policies and procedures for recruitment and termination of employment including initiating the instruction to remove access
- Corporate IT: Responsible for implementing and maintaining internal network security and access control requirements

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by SnapComms. Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the SnapComms production network. Once stored in the environment, the data is accessed remotely from customer systems via the internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

SnapComms has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Encryption is enabled for data stores housing customer data.

Processes, Policies and Procedures

Policies and procedures are in place and include the automated and manual procedures involved in the operation and maintenance of SnapComms. These include those relating to product management, engineering, technical operations, security, and information technology (IT). These procedures are drafted in alignment with the overall information security policies and include Business Continuity, Vulnerability Management, Vendor Management, Physical Security, Operations Security, Asset Management, Cryptography, Access Control, and Acceptable Use. All policies are updated and approved as necessary for changes in the business, but no less than annually. All teams are expected to adhere to the Everbridge and SnapComms policies and procedures that define how services should be delivered. These are located on SnapComms' shared drive and Everbridge intranet and can be accessed by any SnapComms team member.

The following table details the procedures as they relate to the operation of SnapComms:

Procedure	Description
Access Control	How SnapComms restricts logical access, provides and removes that access, and prevents unauthorized access.

Procedure	Description
Operating Procedures for Information and Communication Technology (ICT)	How SnapComms manages the operation of the system and detects and mitigates processing deviations, including logical security deviations.
Change Management	How SnapComms identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How SnapComms identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.
Secure Development	How SnapComms defines rules to ensure that information security is taken into account throughout the entire development life cycle, resulting in secure software and systems.
Cryptographic Controls	How SnapComms ensures the proper and effective use of cryptographic controls in order to protect the confidentiality, authenticity, and integrity of information.
Business Continuity	How SnapComms establishes the steps necessary to implement business continuity management for the SnapComms product.

Physical Security

Everbridge Head Office (Burlington, MA) and SnapComms Office (Auckland, New Zealand) have physical security measures that are designed to deny unauthorized access to equipment, resources ,and to protect personnel and property from damage or harm.

The organization’s sensitive areas are secured via door locks, keycard access controls, physical intrusion detection systems, visitor access control procedures, employee ID badges, and video surveillance systems. SnapComms uses keycard access control systems and badge readers to restrict access to its facilities, and these employee badges and key cards are assigned to personnel using the principle of least privilege.

The company manages its surveillance systems, access controls systems, and alarms. The organization’s facilities are monitored by security surveillance camera systems, with cameras monitoring all ingress and egress points and sensitive areas.

Visitors to the facilities are required to complete an entry in its visitor logs, which document all relevant details regarding the visitor.

Logical Access

Access Control

The onboarding process is initiated by the People and Culture team after the employee completes a successful background check. User accounts are provisioned by SnapComms IT team according to SnapComms’ Access Control Policy.

Each user has a unique identifiable user account. Access to all systems, networks, services, and information is forbidden unless expressly permitted to individual users or business roles. Password complexity is managed in accordance with SnapComms’ Access Control Procedure as part of the Information Security Management System (ISMS) and multi-factor authentication (MFA) is required for all users.

Privileged user access

A privileged user has access to make changes to the production environment. Privileged access rights are restricted and controlled. Privileged rights are allocated to users for ongoing access (on a need-to-use basis) or for temporary access (on an event-by-event basis).

Privileged access is granted:

- To the infrastructure management role that requires it
- Temporarily, during an event which requires the delegation of access (e.g., a security incident which needs prompt investigation)

Requests for new privileged access must be made to the asset owner in writing so that a record is kept. All privileged logins into the production environment are logged.

Requests for new privileged access must be made to the asset owner in writing so that a record is kept. The asset owner approves access based on the above guidelines and, if in doubt, consults the Information Security Manager (ISM). All privileged access to assets, other than by the asset owner, must be recorded by the asset owner or ISM, including any changes to privileged access (addition or removal).

User Account Revocation

Upon termination of employment or an external party contract, the People and Culture Department immediately initiates the removal of all access rights granted to the party in question to avoid unauthorized access by ex-employees or ex-contractors. The following is performed when revoking user access:

- Collecting physical assets allocated to the user (e.g., laptop, office key)
- Removing access to the password management system
- Removing application user accounts by their asset owners
- Removing or suspending the user's user ID (e.g., e-mail address)
- Updating access right records to reflect the changes
- Changing passwords to accounts that will remain active and are know by the departing party

User Access Review

SnapComms reviews user access rights quarterly. When these events are triggered, the employee account is checked for any irregularities in access rights, and access rights are amended or removed, as necessary.

When reviewing the access rights of an asset, the asset owner should consider:

- Whether the current users' access rights match their current role and access profile
- If redundant user access is removed
- Whether privileged access that is no longer needed is removed

Network Access

When considering logical access to SnapComms systems, SnapComms differentiates between the corporate office network and the hosted (cloud) infrastructure. There is no permanent connection between the office and the cloud infrastructure, and logical access to these networks is managed independently.

Cloud Infrastructure Access

The cloud infrastructure has been divided into development, staging, and production subscriptions. The subscriptions serve as permission boundaries and resources from one subscription cannot access resources in another subscription. Permission is assigned as described in the Access Control section above. Logical connectivity is controlled by a combination of internal protocol (IP) address filtering and authentication.

Wherever possible, SnapComms uses PaaS products where the security of the operating system is managed by the hosting provider.

Computer Operations - Backups

Azure is responsible for the backup controls for the in-scope system. Refer to the Subservice Organizations section for additional information.

Computer Operations - Availability

The availability category refers to the accessibility of the system or services as committed by SnapComms' MSA. SnapComms is dependent on many aspects of SnapComms' operations. The risks that would prevent SnapComms from meeting its availability commitments and requirements are diverse. Availability includes consideration of risks during normal business operations, during routine failure of elements of the system, as well as risks related to the continuity of business operations during a natural or man-made disaster.

SnapComms has designed its controls to address the following availability risks:

- Insufficient processing capacity
- Loss of processing capability due to a power outage
- Loss of communication with user entities due to a break in telecommunication services
- Loss of key processing equipment, facilities, or personnel due to a natural disaster

In order to mitigate any identified availability risks, SnapComms uses Azure's PaaS services to ensure that every component of SnapComms' infrastructure is fault tolerant and resilient.

Azure and other external tools continually monitor the system and send alerts to the technology teams when configured thresholds are exceeded. This can assist in ensuring that capacity is sufficient for the number of customers.

Change Control

To mitigate risks associated with changes, SnapComms team implements formal change management responsibilities and procedures to ensure that significant changes to key systems and the production environment is controlled and managed effectively.

Changes to Operational or Production Systems

Changes to operational or production systems must:

- Be approved through the change control process or deployment approval process to ensure justification for business and mitigate potential negative security impacts
- Be communicated by the relevant system owner or end user technologist to their respective cloud service customers (for changes that affect cloud services)
- Be implemented by the SRE Team or by deployment automation with appropriate testing
- Have approvals documented in Jira or in source control
- Have change notifications documented in Slack

The SnapComms Engineering teams working on the SnapComms product follow the SnapComms Secure Development Procedure, which is intended to embed secure processes and practices into the development culture of the organization. This is done to ensure that information security is accounted for at every phase of the development life cycle, and, as a result, the software and systems produced have a high level of security.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Administrative access to the firewalls are restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

In-scope workstations are protected by virus protection software. The software is configured to perform updates to the list of known threats and to protect data from infection by malicious code or viruses in real time.

Penetration testing is conducted annually to identify vulnerabilities in the environment.

Vulnerability scanning is performed by Veracode on a weekly basis.

Boundaries of the System

The scope of this report includes the SnapComms Platform performed in the Auckland, New Zealand, and Everbridge Head Office in Burlington, Massachusetts.

The scope of this report does not include the cloud hosting services provided by Azure at multiple facilities.

Changes to the System in the Last 12 Months

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

Incidents in the Last 12 Months

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

Criteria Not Applicable to the System

All Common/Security, Availability and Confidentiality criterion was applicable to the SnapComms Platform.

Subservice Organizations

This report does not include the cloud hosting services provided by Azure at multiple facilities.

Subservice Description of Services

SnapComms uses Azure as a subservice organization for PaaS provider. Complementary Subservice Organization Controls are expected to be in place at Azure related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. Azure's physical security controls mitigate the risk of unauthorized access to the hosting facilities. Azure's environmental protection controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Complementary Subservice Organization Controls

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

The following subservice organization controls have been implemented by Azure to provide additional assurance that the trust services criteria are met:

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.1	Logical segregation to restrict unauthorized access to other customer tenants is implemented.
		External access to Azure services and the customer data stored in the service requires authentication and is restricted based on customer configured authorization settings.
		All unused IO ports on production servers that reside in edge locations are disabled through the configuration settings at the OS-level.
		Production servers that reside in edge locations are encrypted at the drive level.
		Azure platform components are configured to log and collect security events.
		User credentials adhere to established corporate standards and group policies for password requirements: • Expiration • Length • Complexity • History Initial passwords have secure mechanisms in place for distribution and first-time use. For production domains where passwords are not in use, multi-factor authentication is enforced.
		Administrative access to the Service environment is controlled through defined interfaces that require authentication using appropriate credentials. Privileges (i.e., read, write) are restricted to authorized personnel through designated channels based on job responsibilities.
		Access to production resources requires the use of a Secure Admin Workstation (SAW) which requires MFA for access. SAWs are hardened and secured devices with restricted access.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
		Customer credentials used to access Azure services meet the applicable password policy requirements. Temporary credentials assigned to users by the service expire within 14 days and users are forced to change these credentials when using them for the first time.
	CC6.4; CC7.2	Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established.
		Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		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.
		The datacenter facility is monitored 24x7 by security personnel.
	CC6.5	Guidelines for the disposal of storage media have been established.
	CC6.7	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.
	CC7.2	Azure platform components are configured to log and collect security events.
		Procedures to evaluate and implement Microsoft-released patches to Service components have been established.
		Customer credentials used to access Azure services meet the applicable password policy requirements. Temporary credentials assigned to users by the service expire within 14 days and users are forced to change these credentials when using them for the first time.
	CC8.1	Procedures to evaluate and implement Microsoft-released patches to Service components have been established.
		Azure has established baselines for OS deployments. Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
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.
		Procedures for continuity of critical services provided by third parties have been established. Contracts with third parties are periodically monitored and reviewed for inconsistencies or non-conformance. Procedures to transition between critical third parties based on results of monitoring are established.
		A Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for mapping processes to pre-defined enterprise functions, establishing recovery strategies as well as developing and conducting test scenarios that enable the BCM program to mitigate risks and vulnerabilities and respond to major disruptive events.
		A Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption at least annually. The 'Business Continuity Management Exercise and Test Program Framework' document establishes the basis and process for exercising and testing of the plans for continuity and resumption of critical datacenter processes.
		Datacenter Management teams conduct and document a resiliency assessment, specific to the datacenter's operations, on an annual basis or prior to proposed significant changes.
		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.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
		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.
		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.
		Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities.
		Data corresponding to Azure is backed up to another region other than the primary data location and retained as per the retention policy.
		Production data on backup media is encrypted.
		Azure services are configured to automatically restore customer services upon detection of hardware and system failures.
		Customer data is retained and removed per the defined terms within the Microsoft Online Services Terms (OST), when a customer's subscription expires, or is terminated.
		Datacenter Management team maintains and tests datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.

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

- Communicating with vendors and subservice organization(s) to monitor compliance with the service agreement and stay informed of changes planned at the hosting facility and relay any issues or concerns to Azure management
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring the services performed by vendors and subservice organization(s) to determine whether operations and controls expected to be implemented are functioning effectively

COMPLEMENTARY USER ENTITY CONTROLS

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

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

1. User entities are responsible for having policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by SnapComms according to contractually specified time frames.
2. User entities are responsible for controls to provide reasonable assurance that SnapComms is notified of changes in user entity vendor security requirements and authorized users list.
3. User entities are responsible for having policies and procedures to inform their employees and users that their information or data is being used and stored by SnapComms.
4. User entities are responsible for having policies and procedures to determine how to file inquiries, complaints, and disputes to be passed on to SnapComms.
5. User entities are responsible for granting access to SnapComms' system to authorized and trained personnel.
6. User entities are responsible for controls to provide reasonable assurance that policies and procedures are deployed over user identifications (IDs) and passwords that are used to access services provided by SnapComms.
7. User entities are responsible for deploying physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.