Agora's SOC 2 Examination – Executive Summary

Overview

Agora is a video, voice, and live interactive streaming platform service provider, helping developers deliver rich in-app experiences—including embedded voice and video chat, real-time recording, interactive live streaming, and real-time messaging. Its services support in System as a Service (the "SaaS") model with its owned technology for real-time transmission to achieve high quality and reliable real-time voice and video transmission. Agora supports many customers that span across a broad range of products and services, geographies, and industries.

It is concludes that Agora's information security practices, policies, procedures, and operations meet the SOC 2 standards for Security, Availability, Confidentiality, and Privacy.

Service Provided that In Scope of Examination

Agora is designed to meet trust services criteria relevant to security, availability, confidentiality, and privacy (the "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). The following Agora services are in scope for this report:

Product	Service/Offering	January 1, 2021 to June 30, 2021
Voice Call	Add real-time crystal-clear voice chat into any application with our easy-to-embed SDK	✓
Video Call	Embed real-time high quality video chat and group chat into any app with our easy-to embed SDK	✓
Live Interactive Audio Streaming	Add real-time live interactive audio streaming into any application using our easy-to-embed SDK	✓
Live Interactive Video Streaming	Add real-time live interactive video streaming into any application using our easy-to-embed SDK	✓
Real Time Messaging	In-app chat room, notifications, call signalling and more. Global low latency and high concurrency	✓
Recording	Agora's cloud or on premise local recording solutions	✓
Agora Analytics (Data analytics tool)	Keep track of voice and video chat quality in your apps using our interactive dashboard	✓
SD-RTN	Software Defined Real-time Network	✓

Service Provided by Subservice Organization that Excluded From the Scope of Examination

Agora's controls related to the Agora service detailed in this report cover only a portion of overall internal control for each user entity of Agora. It is not feasible for the Agora service related control criteria to be achieved solely by Agora. Therefore, in conjunction with Agora' controls, a user entity must take into account the related Complementary Subservice Organization Controls expected to be implemented at the Subservice Organizations as follows.

Type of Services Provided	Service Name	Complementary Subservice Organization Controls
Platform as a Service / Infrastructure as a Service	AWS Cloud Services	AWS Cloud is responsible for maintaining controls over access management (including authentication) to the cloud services supporting Agora. Additionally, for services using AWS Cloud, AWS Cloud is responsible for maintaining controls over: • Secure transmission, handling, and storage of data (including encryption, backups, replication, and recovery). • Security, incident, and vulnerability management.
Platform as a Service / Infrastructure as a Service	Alibaba Cloud Services	Alibaba Cloud is responsible for maintaining controls over access management (including authentication) to the cloud services supporting Agora. Additionally, for services using Alibaba Cloud, Alibaba Cloud is responsible for maintaining controls over: • Secure transmission, handling, and storage of data (including encryption, backups, replication, and recovery). • Security, incident, and vulnerability management.
Infrastructure as a Service	IDC Services	IDC Service organizations are responsible for maintaining controls over physical access to the facilities supporting Agora, including data centers. Additionally, IDC Service organizations are responsible for maintaining controls over: • Environmental threats (including natural disasters and man-made threats) • The protection of network equipment (including firewalls and other devices). • Security, incident, and vulnerability management.

Control Environment

Integrity and Ethical Value

Corporate governance at Agora starts with a Board of Directors that establishes, maintains, and monitors standards and policies for ethics, business practices, and compliance that span the company. Corporate governance at Agora shares four core values including:

- Strictly complying with laws and regulations;
- Maintaining the good working environment;
- Duty-bound to safeguard the company's interests; and
- Respecting and protecting the information security.

Agora has appointed a compliance officer to be responsible for the monitoring, interpretation of the standards and policies, and internal communication. The compliance officer designs and provides reports to the Board of Directors on compliance matters. Employees are able to consult with the compliance officer about their concerns, which helps internal communication and understanding of integrity and ethics.

Corporate Governance and Oversight

The control environment reflects Agora's management and employee's attitudes and awareness of internal control activities. It has impacts on the importance of control activities to the organization and how much attention employees pay on the organization's policies, procedures and internal control activities. Agora is led by chief executive officer. Agora's organizational structure and its divisions are defined. The roles and responsibilities of each division are assigned to divisions at organizational level. The reporting line of each division and the corresponding people within a division is available on group information portal to all internal staff to ensure the efficiency of operation and segregation of duties.

Agora security division is responsible for building its security framework against the ISO27001 Information Security Management Standard. The data security committee of security division is responsible for making decision. The data security team of security division is responsible for monitoring. The data security officer team of security division is responsible for compliance management, risk assessment, log audit, external communication, application security, incident management, system maintenance, policies development, architecture security, patch management, vulnerability test, and penetration test. The data privacy officer of security division is responsible for privacy compliance, data classified protection and personal information protection.

Training

Agora follows company's hiring, on-boarding and training program for its employees. The Human Resources Department conducts background checks on prospective employees who meet specific criteria. Specific background checks, such as work experience and personal credit information, are carried out for different levels of prospective employees. All new employees are required to sign confidentiality agreements.

All new employees are required to attend trainings that cover company culture, core values, ethics, code of conduct, information security awareness, security incident handling, and privacy protection. Professional trainings via an online learning platform, email notification, and communication meetings held by internal and external senior experts are available to employees.

Security

Information Security Governance

Agora has established policies and procedures for governing and managing information security and IT operation risk to address security concerns and to coordinate company-wide security initiatives. These policies are able to provide guidance to all departments and personnel for their daily work and management procedures. All policies are available on Agora's internal platforms for employees' reference.

User Access Management

Agora has established Access Control Policy that provides guidance for employees to follow. The Access Control Policy requires following the rules of least privileges and segregation of duties in order to ensure that access to resources and systems within Agora's environment has been properly managed and restricted.

Agora standardizes the process of granting and modifying user access, during which, the management approval is required and the granted access should be commensurate with user's assigned duties. Besides, segregation of duties is required to be concerned to avoid the critical conflicts resulting in risks of material misstatement. The privileged-level access should be restricted to the specific employees according to the principle of matching authority and responsibility.

The good interaction between Agora systems simplifies the access disabling process. As for the in-scope systems except cloud consoles, the user access would be disabled automatically when the HR Department disables the users' IAM account. The access permission to cloud consoles is disabled according to the email notification of the Business Teams or HR Department.

Agora requires conducting yearly access review for the users' permissions and responsibilities. Review results are documented in detail and inappropriate permissions are modified in a timely manner to prevent improper user access.

Logical Security Management

Agora imposes strict password strategies to achieve logical security goals. Agora requires users to set up a password that meets the password requirements including password length, password complexity, maximum login attempts, and change of initial password. In addition, to access the Agora IAM system, employees must pass two-factor authentication based on IAM account name, password, and dynamic digital token received on registered devices.

Network and Infrastructure Management

Agora uses AWS Cloud, Alibaba Cloud Services, and Internet Data Center Services (the "Subservice Organizations") for its network devices, system data storage, and hosting of physical servers.

Agora enables Multi-Factor Authentication (MFA) to secure access to Alibaba Cloud and AWS Cloud consoles. Agora enables the intrusion detection and prevention services to detect mainstream Trojan viruses, blackmail software, DDoS attacks, website backdoors, and other malicious network behaviors for protecting the network security.

Agora rents over two hundred Internet Data Centers (IDCs) as communication nodes. The servers in IDCs are equipped with the baseline configuration and checked for security configuration quarterly. Furthermore, Agora sets up a real-time monitoring system for IDC servers' capacity and traffic, and appoints the Security Team to deal with alarms as well as addressing problems. Agora's all production servers can only be accessed through the bastion host and two-factor authentication is required when logging onto the bastion host. All activities performed in production servers through the bastion host are logged and retained for at least six months. In addition, the logs cannot be modified.

Incident Management

The Agora Incident Response Policy and support procedures provide guidance for employees in monitoring, documenting, escalating, and resolving of problems affecting offered service. These procedures include severity level definitions, escalation procedures, ticket handling procedures, and response time requirements for service alerts.

Agora continuously monitors and analyzes log events to gain a comprehensive view of the security state of the production environment. The logging covers both successful and unsuccessful security events, with an emphasis on the event data of critical infrastructure.

Agora uses the centralized ticketing system to track the identified issues during log event monitoring and the customer feedback of security incidents.

Threat & Vulnerability Management

Agora's threat and vulnerability management ensures the security of Agora and its customers' environments by detecting system flaws and unauthorized actions and taking remediation or mitigating actions on a timely basis. Agora has established Agora Information Security Incident Response System Guideline to regulate security vulnerability management, including classification of security vulnerabilities and response mechanism.

Security incidents and vulnerabilities could be detected via multiple channels, including internal incidents inspection, internal vulnerability scan and external feedback through the official channel of Agora.

Security incidents and vulnerabilities collected via the above channels are gathered into the security incident and vulnerability management platform. The security team reviews the incidents and vulnerabilities on a daily basis to verify the authenticity of the reported incidents and vulnerabilities. Once the security incidents and vulnerabilities are confirmed, the security team will initiate the incident response process and appoints appropriate personnel for resolution. The incident response team will rate, prioritize, and schedule the security incidents and vulnerabilities for resolution. Meanwhile, customers are promptly notified of security issues through online announcements.

The security team has established configuration baseline standards, which specify baseline requirements for operating systems, database management systems, network devices, and virtual images. Configuration baseline standards are reviewed and updated at least once a year by the security team. Configuration scanning tool has been deployed by Agora to scan configurations of operating systems, database management systems, network devices, and virtual images quarterly. The scanning results are analyzed and any deviations from configuration baseline standards will been rectified by operation personnel in time.

The security team conducts the monthly vulnerability scan for all production servers used by Agora. According to the monthly scan results, the security team will classify the problems by severity and assign appropriate specialists to solve them. Besides, Agora has engaged with external vendor (Trustwave) to conduct network penetration test once a year.

Data

Data Storage

Agora provides customers with the Agora On-premise Recording SDK and Agora Recording, enabling customers to record part or all of the call contents. When using the recording services, all recorded video or voice files are stored on the storage server provided by the customer. Agora does not store any streaming data or user data except for caching for transmission purpose. The cached streaming data of users will be immediately released after the service.

Data Availability

Large and distributed data centers: Agora has multiple data centers providing services globally, and attacks on one data center cannot affect another.

Rapid recovery: When a data center is subjected to malicious attacks that are difficult to prevent, such as a distributed denial-of-service (DDOS) attack, Agora will automatically isolate the data center to avoid affecting users' services.

DDOS attack prevention: Agora has deployed anti-DDOS firewalls in each core cloud data center. Agora has more than two hundred distributed data centers around the world, which guarantees sufficient capabilities and resources to control the risk of DDOS attacks.

Data Transmission and Encryption

The communication between the user and the Agora server is protected by transmission protocols, such as the Agora private transmission protocol, Transport Layer Security (TLS) and Web Socket Secure (WSS). Customers can also use Advanced Encryption Standard (AES) or a customized encryption algorithm for the encryption of voice and video data.

During data transmission, the Agora SD-RTN™ does not transmit any encryption key information. Call content information can only be decrypted on the terminal device (such as the client app and the customer's on-premise recording server) through the client authorization key.

Data Backup and Business Continuity Management

Agora uses AWS backup service for automatic data backup every day and the backup data will be retained for a week. Agora also uses Alibaba Cloud backup service, and the jobs are set to perform full cycle of backups of data and logs four times a week. The backup data will be retained for a week. In cases of backup errors or failures, a full backup job cycle will be performed again until the backup succeeds.

Agora defines the backup recovery test procedures and requires restoring the critical data on a yearly basis. The backup data integrity checks are required during the backup recovery process.
Agora established the Business Continuity Plans (BCP) for critical services. For system recovery and reconstitution to a known state per defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), BCP provides roles, responsibilities, and detailed procedures. Plans are reviewed on an annual basis, at a minimum.

Privacy

Privacy Governance

Agora has appointed professionals within the company as Data Protection Officers (DPOs) and assigned personal data protection responsibilities in different service areas. Agora currently implements the personal data protection strategies of the data lifecycle, underpinned by the data security system.

Agora has established the Privacy Policy and required all users and potential users of Agora console to view and accept the terms and conditions of Privacy Policy before registering. The policy defines how Agora would collect, store, and process the Personal Information, and the requirements to be complied by the vendors.

Adoption of Protection Measure

Agora does not store client voice, video, or message data, except for specific storage or caching service. There are three main personal data categories that Agora collects or retains:

- System log covering both the clients' and end users' equipment and network information;
- Online messages cached from the Real-Time Messaging service and the recorded video cached from the Real-Time Recording service; and
- Client contact information for Agora's website service registration.

Agora has categorized and classified personal data collected and retained according to regulatory requirements and the sensitivity of personal data. DPOs have defined standard procedure for internal and vendor to comply in aspect of personal data (1) Storage; (2) Processing; (3) Transmission, and (4) Sharing.

Complementary User Entity Controls

The Applicable Trust Services Criteria cannot be solely and effectively met by the controls of Agora. Agora service is designed with the assumption that certain controls are in operation within the user entity organizations. This section describes those controls that should be in operation at user entity organizations. These Complementary Controls should therefore be considered and developed by user entities. The following list contains controls that customers may need to implement to meet the Applicable Trust Services Criteria which can only be met if Complementary Controls are suitably designed and operated effectively. Each user entity organization must evaluate their own internal control set to determine whether the controls are designed appropriately and operated effectively. The table below is not and does not purport to contain a complete listing of the controls that provide a basis for user entities. In order to achieve effective management, user entities may also need to introduce other control activities where necessary per their specific cases.

Relevant SOC2 Criteria	Domain	Complementary User Entity Controls
CC6.0	Agora Console	User entities approve the nature and extent of user-access privileges for new and modified user access, including standard

Relevant SOC2 Criteria	Domain	Complementary User Entity Controls
		application profiles/roles, critical financial reporting transactions, and segregation of duties.
	Agora Console	User entities should implement appropriate control to ensure that access for terminated and/or transferred users is removed or modified in a timely manner.
	Agora Console	User entities should implement appropriate control to ensure that user access is periodically reviewed.
	Agora Console	User entities should implement appropriate control to ensure that segregation of duties is monitored and conflicting access is either removed or mapped to mitigating controls, which are documented and tested.
	Agora Console	User entities should implement appropriate control to ensure that privileged-level access (e.g., security administrators) is authorized and appropriately restricted.
	Agora Console	User entities should use multi-factor authentication to access Agora console. The selection of “allow agora workers to operate console” need to be configured to “not allow”.
CC6.0	User entities data related to use Agora service	a. User entities should establish appropriate backup and restoration strategy and plan according to their needs. These should be tested to ensure its effectiveness. b. User entities should establish disaster recovery plan and business continuity plan according to their needs. The drill test should be performed periodically. c. User entities should utilize multi-zone and multi-region options, and design and implement redundant systems to ensure a desired level of redundancy and a high availability architecture.
CC8.0	SDKs	User entities are responsible for testing and approving application changes before being moved into the production environment when embaying the SDK or API service.
	SDKs	User entities should implement appropriate control to ensure that access to implement changes into the application production environment is appropriately restricted and segregated from the development environment.
C (Additional Criteria for Confidentiality)	User entities application	User entities should use built-in AES 128/256 support provided by Agora or third-party encryption to protect all data transmitted between the end user and Agora services.
P1/P2 (Additional Criteria for Privacy)	Agora Console-Privacy	User entities should check the customer agreement and privacy notice website frequently for any changes.
		User entities are responsible for managing disclosure and notice requirements for personal information they collect from users and themselves

Relevant SOC2 Criteria	Domain	Complementary User Entity Controls
P3/P4 (Additional Criteria for Privacy)	Agora Console-Privacy	User entities are responsible for complying with any regulations or laws that require a rationale of the purposes for which personal information is collected, used, retained, and disclosed.
P5 (Additional Criteria for Privacy)	Agora Console-Privacy	User entities are responsible for providing individuals with their person information, if required to do so by law.
P7 (Additional Criteria for Privacy)	Agora Console-Privacy	User entities are responsible for keeping accurate and complete personal information.