KRONOLOGIC

Service Organization Control 3 (SOC 3®) Report

Kronologic's report on its Kronologic App relevant to Security for the period
September 1, 2020 to February 28, 2021

Attestation & Advisory Services

MHM
Professional Corporation
Chartered Professional Accountant

Table of Contents

Section I

Kronologic's Management Assertion

Kronologic's Management Assertion

We are responsible for designing, implementing, operating and maintaining effective controls within Kronologic's ("Kronologic") Kronologic App ("system") throughout the period September 1, 2020 to February 28, 2021, to provide reasonable assurance that Kronologic's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in attachment A 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 September 1, 2020 to February 28, 2021, to provide reasonable assurance that Kronologic's service commitments and system requirements were achieved based on the trust services criteria relevant to security (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*). Kronologic's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

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 September 1, 2020 to February 28, 2021, to provide reasonable assurance that Kronologic's service commitments and system requirements were achieved based on the applicable trust services criteria.

Christopher Lee
Christopher Lee (Apr 5, 2021 13:18 CDT)

Chris Lee
Chief Technology Officer
April 5, 2021

Section II

Independent Service Auditor’s Report

Independent Service Auditor’s Report

To the Management of Kronologic:

Scope

We have examined Kronologic’s (“Kronologic”) accompanying assertion titled "Kronologic's Management Assertion” (“assertion”) that the controls within the Kronologic App (“system”) were effective throughout the period September 1, 2020 to February 28, 2021, to provide reasonable assurance that Kronologic’s service commitments and system requirements were achieved based on the trust services criteria relevant to security (“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*).

Service organization's responsibilities

Kronologic is responsible for its service commitments and system requirements and for designing, implementing and operating controls within the system to provide reasonable assurance that Kronologic’s service commitments and system requirements were achieved. In Section I, Kronologic has provided the accompanying assertion titled "Kronologic's Management Assertion” (“assertion”), about the effectiveness of controls within the system. When preparing its assertion, Kronologic 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 auditors’ responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management’s assertion that controls within the system were effective throughout the period to provide reasonable assurance 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 American Institute of Certified Public Accountants (AICPA) and Canadian Standard on Assurance Engagements 3000, Attestation Engagements Other Than Audits or Reviews of Historical Financial Information, set out in the *CPA Canada Handbook – Assurance*. These 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
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Kronologic's service commitments and system requirements based on the applicable trust criteria
- Performing such other procedures as we considered necessary in the circumstances

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 achieve the service organization's service commitments and system requirements based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the Kronologic Kronologic App were effective throughout the period September 1, 2020 to February 28, 2021, to provide reasonable assurance that Kronologic's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Restricted use

Certain complementary subservice controls that are suitably designed and operating effectively are necessary, along with controls at Kronologic, to achieve Kronologic's service commitments and system requirements based on the applicable trust services criteria. Users of this report should have sufficient knowledge and understanding of complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements. Kronologic uses Amazon Web Services (AWS) to provide cloud infrastructure services. Users of this report should obtain the relevant AWS SOC2 or SOC3 report.

MHM Professional Corporation

Chartered Professional Accountant
Calgary, Alberta
April 5, 2021

Attachment A

Kronologic's Description of the Boundaries of its Kronologic App

Kronologic's Description of the Boundaries of its Kronologic App

Types of Services Provided

Kronologic is a privately held technology company founded in 2018 and headquartered in Austin, Texas. Kronologic is the Kronologic App for the enterprise. The application automates the sending of meeting invites triggered by CRM integrations and manual list uploads. The solution enables knowledge workers like marketing, sales, and customer success to set revenue generating meetings at scale.

The Kronologic App automates the sending of meeting invites and utilizes built in AI that negotiates alternative times on behalf of the user using a natural language processor or through the calendar's own rescheduling functions. This is accomplished with no human effort. Messaging workflows manage the sequence, timing, copy, lead routing, and CRM field updates for continued actions beyond the sequence. The application also includes extensive reporting options for teams, individuals and campaigns: meeting disposition, meetings booked, meeting forecasting, value per meeting, meeting type effectiveness, campaign effectiveness, and meeting invite status.

The Kronologic App is a SaaS solution that includes a web-based user interface for customers to track calendar invites and acceptance and load email for potential sales leads. Customers have the ability to define the frequency of invites, times of day, messages, and sales targets. Companies of all sizes now use Kronologic to maximize their bookings and revenue.

The Boundaries of the System Used to Provide the Services

The boundaries of the system are the specific aspects of Kronologic's infrastructure, software, people, procedures and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures and data that indirectly supports the services provided to customers are not included within the boundaries of the system.

The components that directly support the services provided to customers are as described in the sections below.

Infrastructure

Kronologic is a SaaS-multi-tenant client-server application hosted in Amazon Web Services (AWS). All customers receive their own data partition in the Kronologic App, and their data is logically separated and not accessible to other tenants preventing unauthorized access.

The Kronologic application runs within an AWS Virtual Private Cloud (VPC) which is hosted in the US east region and spans two availability zones with Amazon Linux 2 as the operating system.

The database supporting the application utilizes AWS RDS running Postgres. The primary database resides in the US east region and is replicated real-time into a replica instance in a separate availability zone for backup and redundancy purposes. Coralogix is used for both monitoring and log storage.

Software

The following provides a summary of software systems used to deliver the Kronologic App:

- Coralogix – used for the monitoring of production systems and log storage.
- Coralogix / AWS Cloudwatch – used for enterprise monitoring of availability and capacity.
- Rapid7 Insight – used for web application vulnerability scanning.
- Gitlab – used for source code version control.
- Linux 2 – operating systems to support operation of the system.
- Go – programming language used to write the backend API of the web application.
- Gmail/Microsoft O365 - used for sending application email

People

Kronologic has a defined organizational structure with specific roles, responsibilities, and appropriate lines of reporting required to support the Kronologic App. It is comprised of, and supported by, the following teams who are responsible for the delivery and management of the system:

- Management – responsible for providing the overall direction, strategic vision, and management of Kronologic.
- Product – responsible for guiding the overall direction of the product roadmap including usability, enhancements, and new features.
- Engineering – responsible for front and back-end development of the in-scope applications and services. Also, responsible for oversight of software and data engineering, IT Infrastructure, and all IT related activities.
- Finance & Accounting – responsible for company finance and accounting aspects.
- Sales – responsible for development of new business related to the Kronologic services.
- Customer Success - responsible for successful onboarding of customers on Kronologic platform and act as advocates for the continued success of the platform. They are responsible for product support issues, customer engagement and growth
- Marketing - responsible for marketing and advertising of the product.

The teams and associated initiatives, workstreams, and functions are led by the executive management leads.

Procedures

Management has developed and communicated to employees and contractors a set of policies, processes, and procedures in several operational areas which support the security, availability, and confidentiality objectives of the Kronologic App. As part of the wider Information Security Management Program, Kronologic has developed and organized the following policies and procedure documents that are used to support the Kronologic App.

The following policies and procedures are reviewed annually or after significant business changes by the Kronologic Policy Compliance Committee. Policies and procedures are accessible by employees and contractors through internal document repositories:

- Access Control
- Application Security
- Asset Management
- Incident Response
- Information Security
- Problem Management
- Vulnerability Assessment & Threat Management
- Risk Assessment
- Business Continuity Plan
- Change Management
- Backup
- Disaster Recovery
- Software Development Lifecycle (SDLC)
- Code of Conduct
- Ethics & Compliance

Control activities have been placed into operation to help ensure that actions are carried out properly and efficiently to achieve policies and procedures compliance. Kronologic has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the applicable trust services criteria and the overall objective of the organization.

Data

Data is entered via the browser application and sent to the application servers via calls to the API. The data is processed and written to a Postgres instance. Data transmission is secured using TLS 1.2, encryption keys in PEM format, SHA-256 (Example - SHA-512) with ECDSA Encryption, and does not leave the VPC. Data replication channels are also encrypted and transmitted via the private AWS managed connection. All data access requests require user and organization authentication and verification. These requests are validated via the Kronologic permissions system to exclude the possibility of cross-client data leakage. All data at rest is encrypted using AES-256 encryption.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Kronologic designs its processes and procedures related to its Kronologic App to meet its objectives. Those objectives are based on the service commitments that Kronologic makes to user entities, the laws and regulations that govern SaaS providers, and the financial, operational, and compliance requirements that Kronologic has established for the services.

Security commitments to user entities are documented in customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Kronologic App that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Use of encryption protocols to protect customer data at rest and in transit.