SOC 3 ® Report

Description of Kronos Incorporated's Kronos Private Cloud (KPC) Infrastructure Services System relevant to Security, Availability and Confidentiality

For the Period November 1, 2018 to October 31, 2019

Table of Contents

Management's Assertion Regarding the Effectiveness of Its Controls Over the Kronos Incorporated's Kronos Private Cloud (KPC) Infrastructure Services System

We, as management of, Kronos Incorporated (Kronos or service organization) are responsible for:

- Identifying the *Kronos Private Cloud Infrastructure Services System* (System) and describing the boundaries of the System, which are presented in the section below titled *System Description of the Kronos Private Cloud Infrastructure Services System*
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in the section below titled *System Description of the Kronos Private Cloud Infrastructure Services System*
- Identifying, designing, implementing, operating, and monitoring effective controls over the *Kronos Private Cloud Infrastructure Services System* (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

Kronos uses Cyxtera Data Centers, Inc. (Cyxtera) and Equinix, Inc. (Equinix) (jointly, Subservice Organizations) to provide data center hosting services consisting of physical security and environmental controls. The Description includes only the controls of Kronos and excludes controls of Cyxtera and Equinix however it does present the types of controls Kronos assumes have been implemented, suitably designed, and operating effectively at Cyxtera and Equinix. The Description also indicates that certain trust services criteria specified therein can be met only if Kronos' controls assumed in the design of Kronos' controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of Cyxtera and Equinix.

However, we perform annual due diligence procedures for third-party sub-service providers and based on the procedures performed, nothing has been identified that prevents Kronos from achieving its specified service commitments.

We assert that the controls over the system were effective throughout the period November 1, 2018 to October 31, 2019, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

The Management of Kronos Incorporated
December 6, 2019

Ernst & Young, LLP
200 Clarendon Street
Boston, Massachusetts 021116

Tel: +01 617 266 2000
Fax: +01 617 266 5843
ey.com

Building a better working world

Report of Independent Accountants

To the Board of Directors
Kronos Incorporated

Scope
We have examined management's assertion, contained within the accompanying Management's Assertion Regarding the Effectiveness of Its Controls Over the Kronos Incorporated's Kronos Private Cloud (KPC) Infrastructure Services System (Assertion), that Kronos Incorporated's controls over the Kronos Private Cloud (KPC) Infrastructure Services System (System) were effective throughout the period November 1, 2018 to October 31, 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, processing integrity and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Management's Responsibilities
Kronos management is responsible for its assertion, selecting the trust services categories and associated criteria on which the its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Kronos Private Cloud (KPC) Infrastructure Services (System) and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- identifying, designing, implementing, operating, and monitoring effective controls over the Kronos Private Cloud (KPC) Infrastructure Services (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement.

Kronos uses Cyxtera Data Centers, Inc. (Cyxtera) and Equinix, Inc. (Equinix) (subservice organizations) to data center hosting services consisting of physical security and environmental controls. The Description of the boundaries of the System indicates that Kronos' controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if Cyxtera and Equinix controls, assumed in the design of Kronos' controls, are suitably designed and operating effectively along with related controls at the service organization. The Description presents Kronos' system and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at Cyxtera and Equinix. Our examination did not extend to the services provided by Cyxtera and Equinix and we have not evaluated whether the controls management assumes have been implemented at Cyxtera and Equinix have been implemented or whether such controls were suitably designed and operating effectively throughout the period November 1, 2018 to October 31, 2019.

Our Responsibilities
Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Kronos' relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls,

Ernst & Young, LLP
200 Clarendon Street
Boston, Massachusetts 021116

Tel: +01 617 266 2000
Fax: +01 617 266 5843
ey.com

and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Kronos' cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations:
Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Kronos' principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion:
In our opinion, Kronos' controls over the system were effective throughout the period November 1, 2018 to October 31, 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria, if the subservice organizations applied the controls assumed in the design of Kronos' controls throughout the period November 1, 2018 to October 31, 2019.

Ernst & Young LLP

December 6, 2019

System Description of the Kronos Private Cloud Infrastructure Services System

Overview of the organization and services

Kronos Incorporated (Kronos) is a global privately held company founded in 1977, based in Lowell, Massachusetts, serving organizations in more than 100 countries, including many Fortune 1000 companies. These organizations use Kronos' time and attendance, scheduling, absence management, human resource, payroll, hiring and labor analytics applications. Kronos is a recognized leader in workforce management solutions that enable organizations to control labor costs and improve workforce productivity.

Kronos' workforce management solutions provide the complete automation and high-quality information Customers need to help control labor costs, minimize compliance risk, and improve workforce productivity. The Kronos solution can deliver continuous value only if it is available and managed properly over time. More Customers are choosing Kronos Cloud Services for hosting and deploying their workforce management solutions.

Kronos provides comprehensive hosting, maintenance, and support of the human capital management solution, including complete support of IT infrastructure encompassing computer hardware, operating systems, and database systems required to run Kronos applications. This service also includes items such as:

- Server security and management
- Service pack installation
- Legislative update installation
- Software version installation
- Disaster recovery capabilities

Scope of the report and overview of the services

The scope of the Description covers Kronos' processes and controls relevant to the design, operation and maintenance of the KPC Infrastructure Services (i.e., network, operating system and database layers) (collectively referred to as "KPC environment") at the following locations:

- Waltham, Massachusetts;
- Chicago, Illinois;
- Frankfurt, Germany; and
- Amsterdam, Netherlands

The Description does not cover the application layer (including end-user authentication) of Customer systems (i.e., the Workforce Central or Workforce TeleStaff front-end applications), as customers are responsible for managing these technology components and thus are not considered part of the Kronos KPC Infrastructure Services System.

Product overview and service

The Kronos Private Cloud (KPC) Infrastructure Services (hereafter referred to as KPC) hosts and manages the infrastructure components of Kronos' workforce management solutions, where customers can access their application(s) over the Web at any time, from anywhere through a front-end interface called Workforce Central. KPC customers receive 24x7 access to their solution without having to purchase additional hardware, operating systems, or database licenses. KPC services provide valuable

peace of mind knowing that experienced Kronos technical consultants are managing their applications and employee data. KPC is the ideal choice for organizations seeking to achieve their workforce management goals without exceeding their capital equipment budgets or placing additional demands on their in-house IT staff.

Components of the system

Infrastructure

The infrastructure supporting the KPC environment is segmented into modular environments referred to as 'pods.' Each pod is bordered by redundant firewall technology, provided by two different vendors, which is responsible for traffic policing and policy enforcement both in and out of the pod, as well as within Layer 2 & 3 network controls. Individual Customer and infrastructure servers, running Windows Servers, are authenticated/authorized through Active Directory membership, group policy enforcement, two-factor authentication and public key cryptography. Customer specific configurations and data are maintained on Microsoft SQL (which are also subject to Active Directory controls and policy) and are themselves isolated on a per customer, per network basis. To support inbound and outbound transmissions, the KPC environment also contains a 'file transfer manager' that uses Secure File Transfer Protocol (SFTP).

Throughout the period, Kronos contracted with an industry recognized data center provider, Cyxtera, that provides data center space, power and connectivity for the infrastructure supporting the KPC environment in the United States. Kronos also contracted with an industry recognized data center provider, Equinix, that provides data center space, power and connectivity for the infrastructure supporting the KPC environment in Europe. As part of the continuous monitoring program, Kronos reviews a copy of the most recent annual service auditor's report for each respective data center.

Software

The applicable software supporting the relevant Kronos products and services includes various utilities that are used by Kronos personnel in managing and monitoring the environment. These utilities include items such as backup and replication, patch management, antivirus and database management software. Access to and use of these utilities is restricted to appropriate personnel who require such access to complete their job responsibilities.

Data

Customer data is held in accordance with applicable data protection and other regulations set out in customer contracts and limits access to electronically held customer data on a least privileged basis. Customer data is held in a database management system, which is managed by the Hosting Operations team. Data in transmission is encrypted using Transport Layer Security (TLS) sessions or SFTP. Access to customer data in the relevant Kronos products is limited to authorized personnel and is granted in accordance with Kronos system security administration policies.

Procedures

Kronos has documented policies and procedures to support the operations and controls over its infrastructure in support of the KPC environment. Relevant policies and procedures are made available to employees through the corporate intranet sites. Control activities in support of these policies and procedures have also been designed.

Service commitments and requirements

Kronos designs its processes and procedures relevant to the Kronos Private Cloud to meet objectives for its Workforce Management and Human Capital Management services. Kronos' objectives are based on the service commitments made to the Customers in relevant contracts, applicable laws and regulations, and the financial, operational and compliance requirements that Kronos has established. The principal service commitments and system requirements commitments include:

- Implementing logical and physical access restrictions to help ensure that logical and physical access to programs, data, and IT resources is restricted to appropriately authorized users and that access is restricted to performing appropriately authorized actions.
- Implementing technical and non-technical controls, along with safeguards, to help ensure the availability of data in accordance with the system documentation and requirements.
- Implementing technical and non-technical controls to retain and dispose of confidential data in accordance with agreed upon retention terms.

Kronos establishes operational requirements that support the achievement of its security, availability, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Kronos' policies and procedures, system design documentations and contracts with third parties (customers and vendors).

Subservice Organization Complementary Controls

Kronos utilizes the following subservice organizations as it relates to the KPC system:

- **Cyxtera and Equinix**: Cyxtera and Equinix (subservice organizations) to provide data center hosting services, including physical security and environmental safeguards, to support the KPC environment.

It is expected that the above organizations have implemented the controls listed below to support achievement of the affected criteria which were communicated to the vendors through the contract acceptance process. Kronos performs due diligence procedures upon engagement and has implemented various monitoring activities to monitor the services provided by Cyxtera and Equinix through their vendor management process which confirms that contractual commitments are being met and effective controls exist over third-party services.

Criteria	Expected subservice organization controls
CC6.4	Access to the data center and its components is restricted to authorized employees and contractors through the use of card readers and other systems (e.g. hand readers).
	Visitors to the data center are required to sign a visitor log.
	Physical access to the data center facilities is restricted to appropriate personnel who require such access to perform their job functions and reviewed on a periodic basis.
	Administrative access to the card system and other systems (e.g. biometric readers) is limited to authorized and appropriate personnel.
	Camera surveillance of the data center is monitored and retained for a period of time.
A1.2	Environmental safeguards at the data center facilities are designed, implemented, operated, and maintained, including the following: • Fire detection and suppression systems • Climate, including temperature and humidity, control systems • Uninterruptible power supplies (UPS) and backup generators • Redundant power and telecommunications lines • Alerts for HVAC elements which are triggered when thresholds have been reached

User Entity Responsibilities

In designing the System, Kronos has contemplated that certain controls would be implemented by user entities to achieve the applicable trust services criteria supporting the System, which were communicated to user entities through the contract acceptance process. The complementary user entity controls presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities.

- User entities are responsible for determining that the functionality within the KPC system meets their requirements and notifying Kronos timely with any required changes or enhancements. (CC2.3)
- User entities are responsible for managing (i.e., user provisioning, user de-provisioning, access reviews) and configuring application logical access (i.e., password settings, multi-factor/two-factor authentication) to help ensure that access remains restricted to authorized and appropriate personnel. (CC6.1, CC6.2, and CC6.6)
- User entities are responsible for communicating security, availability and confidentiality commitments and responsibilities to their internal and external users accessing data within the System and providing users with the resources necessary to fulfill their commitments and responsibilities. (CC2.2 and CC2.3)
- User entities are responsible for adequately securing and disposing of any system output provided by the System. (CC6.6 and CC6.7)
- User entities are responsible for appropriately securing transmissions of data to Kronos, which includes transmissions from middleware, and informing Kronos of any necessary changes to the System. (CC6.7)
- User entities are responsible for implementing processes and controls to prevent and detect unauthorized or malicious software and unauthorized access to the system or activity. (CC6.8)
- User entities are responsible for approving and validating the appropriateness (and maintaining the confidentiality) of data provided to Kronos and any changes to that data. CC6.3
- User entities are responsible for reviewing changes to their data to help ensure that all changes are appropriate and authorized. (CC6.8)
- User entities are responsible for reviewing notifications from Kronos of changes to the KPC environment and communicating any concerns to Kronos. User entities are responsible for ensuring their systems are in compliance with regulatory requirements and state laws, any specific requirements should be communicated to Kronos in a timely manner. (CC2.3 and CC3.1)
- User entities are responsible for communicating any identified incidents impacting the security, availability or confidentiality of the system to Kronos on a timely basis. (CC2.3)
- User entities are responsible for reviewing relevant audit trails and notifying Kronos of any discrepancies or unauthorized activity. (CC1.1)
- User entities are responsible for communicating any changes to their data retention and destruction requirements from the original contract terms to Kronos in a timely manner or setting and reviewing configurable settings related to data retention in the System, where applicable. (C1.1 and C1.2)
- User entities are responsible for maintaining servers supporting the time-clock systems and restricting access to authorized individuals. (CC6.4, CC6.5 and CC6.6)