SOC 3 ® Report

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

For the Period November 1, 2017 to October 31, 2018

Table of Contents

Management's Assertion Regarding the Effectiveness of Its Controls Over the Kronos Private Cloud (KPC) Infrastructure Services System Based on the Trust Services Principles and Criteria for Security, Availability and Confidentiality

Kronos Incorporated ("Kronos") utilizes Cyxtera Data Centers, Inc. (Cyxtera) and Equinix, Inc. (Equinix) (subservice organizations) to provide various data center hosting services to support the Kronos Private Cloud (KPC) Infrastructure Services System.

We, as management of Kronos, are responsible for designing, implementing and maintaining effective controls over the KPC Infrastructure Services System (System) to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in Security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity's security controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are 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.

We have performed an evaluation of the effectiveness of the controls over the System throughout the period November 1, 2017 to October 31, 2018, to achieve the commitments and system requirements related to the operation of the System using the criteria for security, availability and confidentiality (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this evaluation, we assert that the controls were effective throughout the period November 1, 2017 to October 31, 2018 to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve Kronos' commitments and system requirements;
- the System was available for operation and use, to achieve Kronos' commitments and system requirements; and
- the System information is collected, used, disclosed, and retained to achieve Kronos' commitments and system requirements

based on the Control Criteria.

Our attached description of the boundaries of the KPC Infrastructure Services System identifies the aspects of the KPC Infrastructure Services System covered by our assertion.

The Management of Kronos Incorporated

December 10, 2018

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 Management of Kronos Incorporated:

Approach:
We have examined management's assertion that Kronos Incorporated ("Kronos") maintained effective controls to provide reasonable assurance that:

- the Kronos Private Cloud (KPC) Infrastructure Services System was protected against unauthorized access, use, or modification to achieve Kronos' commitments and system requirements;
- the KPC Infrastructure Services System was available for operation and use to achieve Kronos' commitments and system requirements; and
- the KPC Infrastructure Services System information is collected, used, disclosed, and retained to achieve Kronos' commitments and system requirements

during the period November 1, 2017 to October 31, 2018 based on the criteria for security, availability and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100A, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Kronos' management. Our responsibility is to express an opinion 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, 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 and appropriate 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:
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 inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability and confidentiality are achieved.

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

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

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. Furthermore, projections of any evaluation of effectiveness to future periods are 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, Kronos' management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability and confidentiality.

Ernst & Young LLP

December 10, 2018

System Description of the Kronos Private Cloud (KPC) 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 workforce 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

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.

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 Server 2008 or Windows Server 2012 are themselves 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 KPC environment only includes various utilities that are used by Kronos personnel in managing 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 Kronos personnel who require such access to complete their job responsibilities.

Procedures

Kronos has documented policies and procedures to support the operations and controls over its infrastructure systems in support of the KPC environment. Relevant policies and procedures are made available to employees through the corporate intranet sites

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. Access to Customer data is limited to authorized Kronos personnel, and is granted in accordance with Kronos system security administration policies.

Subservice organizations complementary controls

Kronos utilizes Cyxtera and Equinix (subservice organizations) to provide data center hosting services, including physical security and environmental safeguards, to support the KPC environment. Kronos has implemented various monitoring activities to monitor the described 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.

It is expected that the subservice organization has implemented the following controls to support achievement of the associated criteria:

Criteria Reference	Expected Subservice Organization Controls
CC5.5	Access to the data center 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.
	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

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 environment meets their requirements and notifying Kronos timely with any required changes or enhancements. (CC7.3)
- 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. (CC2.3)
- User entities are responsible for securing transmissions of data to Kronos, and informing Kronos of any necessary changes to the System. (CC5.7)
- User entities are responsible for requesting and maintaining Secure File Transfer Protocol (SFTP) user accounts from Kronos and informing Kronos of any changes needed. (CC5.4 and CC5.7)
- 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. (CC5.8)
- 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. (C1.2)
- User entities are responsible for reviewing notifications from Kronos of changes to the KPC environment and communicating any concerns to Kronos. (CC7.4)
- 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. (CC3.3)
- User entities are responsible for communicating any identified incidents impacting the security, availability or confidentiality of the system to Kronos on a timely basis. (CC6.2)
- 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. (C1.7 and C1.8)