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, 2019 to October 31, 2020
# Table of Contents

**Management’s Assertion Regarding the Effectiveness of Its Controls Over the Kronos Incorporated’s Kronos Private Cloud (KPC) Based on the Trust Services Criteria for Security, Availability, and Confidentiality** ................................................................. 1

**Report of Independent Accountants** ........................................................................................................ 2

**System Description of the Kronos Private Cloud (KPC) System** ................................................................. 4

- Product overview and service ....................................................................................................................... 5
- Components of the system ........................................................................................................................... 5
- Service commitments and requirements ...................................................................................................... 6

**Subservice Organization Complementary Controls** .................................................................................. 7

**User Entity Responsibilities** ................................................................................................................... 8
Management’s Assertion Regarding the Effectiveness of Its Controls Over the Kronos Incorporated’s Kronos Private Cloud (KPC) Based on the Trust Services Criteria for Security, Availability, and Confidentiality

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

- Identifying the Kronos Private Cloud (KPC) (System) and describing the boundaries of the System, which are presented in the section below titled System Description of the Kronos Private Cloud (KPC) 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 (KPC) System
- Identifying, designing, implementing, operating, and monitoring effective controls over the Kronos Private Cloud (KPC) 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) to provide hosting services including physical 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’s controls, assumed in the design of Kronos’ controls, are suitably designed and operating effectively along with related controls at the service organization. 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 Cyxtera’s and Equinix’s 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 subservice 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, 2019 to October 31, 2020, 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 4, 2020
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)” (Assertion), that Kronos Incorporated's controls over the Kronos Private Cloud (KPC) System (System) were effective throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, 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) System (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 KPC System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements.

Kronos uses Cyxtera Data Centers, Inc. (Cyxtera) and Equinix, Inc. (Equinix) to provide hosting services including physical 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's 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, 2019 to October 31, 2020.

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, 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, 2019 to October 31, 2020, 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, 2019 to October 31, 2020.

Ernst & Young LLP

December 4, 2020
System Description of the Kronos Private Cloud (KPC) 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

On April 1, 2020, Kronos Incorporated merged with Ultimate Software, a human capital management (HCM) and employee experience solutions provider located in Weston, Florida. As of October 1, 2020, the two companies rebranded to form UKG (Ultimate Kronos Group), an innovative HCM and workforce management company, that solidifies an even stronger position in the HCM marketplace with highly complementary products and a combined 70 years of expertise. Both Kronos Incorporated and Ultimate Software operated independently during the entire reporting period. There were no significant changes to Kronos' control environment during the audit period as a result of the merger.

Scope of the report and overview of the services

This description was prepared in accordance with the criteria set forth for a SOC 2® Type 2 Report in the Kronos Management Assertion and the guidance for a description of a service organization's system set forth in the AICPA Attestation Standards.

The scope of the Description covers Kronos’ processes and controls relevant to the design, operation and maintenance of the Kronos Private Cloud (“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 (e.g., 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
Product overview and service

The KPC Infrastructure Services 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, which run Windows Server operating system, 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 provided 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 provided 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, environment monitoring, 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 Secure File Transmission Protocol (SFTP). Data security is further discussed in section 3.4.6, titled “Data Transmission” and section 3.4.7, titled “Availability” of this report. 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

In support of the environment, Kronos has documented policies and procedures to support the operations and controls over its infrastructure and application systems. 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 and are described in further detail in section 3.4, titled “Overview of Kronos’ control activities.”

Service commitments and requirements

Kronos designs its processes and procedures relevant to the System to meet objectives for its Workforce Management. Kronos’ objectives are based on the service commitments made to the Customers in relevant contracts, applicable laws and regulations. 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.
- Applying technical and non-technical controls to retain and dispose of confidential data in accordance with agreed upon retention terms.
- Ensuring executive oversight and commitment to confidentiality through appointment of roles across the organization that monitor and report on compliance with relevant regulations.
- Instituting governance policy and procedures that collectively represent Kronos’ processes over protecting data and promote staff awareness of data protection processes.
- Executing a vendor risk management process to include oversight and contractual commitments from third parties that are consistent with Kronos expectations.
- Assessing risk continuously as Kronos products and processes evolve, utilizing the Data Inventory and Classification system.

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 documentation 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.

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 organizations have implemented the following controls to support achievement of the associated criteria:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Expected subservice organization controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC2.2, CC7.3</td>
<td>The entity will notify Kronos of any incidents or breaches.</td>
</tr>
<tr>
<td>CC6.1, CC6.2, CC6.3</td>
<td>Controls to address logical access to application software, system software, databases, and network components is restricted to authorized and appropriate users to perform authorized and appropriate actions.</td>
</tr>
<tr>
<td>CC6.1</td>
<td>Controls to address user authentication mechanisms (i.e., passwords).</td>
</tr>
<tr>
<td>CC6.4</td>
<td>Controls to address physical access and environmental protections to computer equipment and storage media are established.</td>
</tr>
</tbody>
</table>
User Entity Responsibilities

The controls at Kronos were designed with the assumptions that certain controls would be implemented by user entities. The application of certain controls by user entities is necessary to achieve the criteria identified in this report.

This section describes certain controls that the user entities should consider for achievement of the criteria identified in this Description. 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. (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 and CC6.8)
- User entities are responsible for reviewing notifications from Kronos of changes to the KPC environment and communicating any concerns to Kronos. (CC8.1)
- 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)