KRONOS®

SOC 3 ® Report

Description of the Workforce Ready Partner Network Infrastructure and Application Services System relevant to Security, Availability, and Confidentiality

For the Period October 1, 2017 to September 30, 2018

Table of Contents

Management's Assertion Regarding the Effectiveness of Its Controls Over the Workforce Ready Partner Network Infrastructure and Application Services System Based on the Trust Services Principles and Criteria for Security, Availability and Confidentiality

Kronos Incorporated ("Kronos") utilizes QTS Realty Trust, Inc. (QTS) and General Datatech, LP (GDT) (subservice organizations) to provide various data center hosting services to support the Workforce Ready Partner Network Infrastructure and Application Services System.

We, as management of Kronos, are responsible for designing, implementing and maintaining effective controls over the Workforce Ready Partner Network Infrastructure and Application 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 October 1, 2017 to September 30, 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 October 1, 2017 to September 30, 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
- 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 Workforce Ready Partner Network Infrastructure and Application Services System identifies the aspects of the Workforce Ready Partner Network Infrastructure and Application Services System covered by our assertion.

The Management of Kronos Incorporated
November 15, 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 Workforce Ready Partner Network Infrastructure and Application Services System was protected against unauthorized access, use, or modification to achieve Kronos' commitments and system requirements
- the Workforce Ready Partner Network Infrastructure and Application Services System was available for operation and use to achieve Kronos' commitments and system requirements
- the Workforce Ready Partner Network Infrastructure and Application Services System information is collected, used, disclosed, and retained to achieve Kronos' commitments and system requirements

during the period October 1, 2017 to September 30, 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

November 15, 2018

System Description of the Workforce Ready Partner Network Infrastructure and Application 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 Workforce Ready Partner Network Infrastructure and Application Services (hereafter referred to as Workforce Ready Partner Network, WFR Partner Network or WFRPN) is a provider of Software as a Service (SaaS) based workforce management applications with a major focus in delivering solutions that support human resources (HR), payroll, and time and labor management. Each solution can be used individually, as a complete suite, or in conjunction with other third-party applications, content, and/or services. Kronos delivers the platform for applications and third-party offerings to be accessed within one interface. The Workforce Ready Partner Network solution is offered to Kronos' customers (Customers) subscribing to one or more of the product's core modules. Workforce Ready Partner Network is available any time, from anywhere through a front-end interface called Workforce Ready Partner Network. Customers of Workforce Ready Partner Network receive 24x7 access to their solution without having to purchase additional hardware, operating systems, or database licenses. Workforce Ready Partner Network provides Customers with valuable peace of mind, knowing that experienced Kronos technical consultants are managing their applications and employee data. Workforce Ready Partner Network is a choice for organizations seeking to achieve their human capital management goals without exceeding their capital equipment budgets or placing additional demands on their in-house IT staff.

Kronos also engages with a third-party subservice organization to provide data center hosting services to the infrastructure supporting the System, with respect to the operating system level. Some of these services include: physical security; environmental safeguards, operating system patching, antivirus management, firewall configuration management, network management, and server provisioning. Per the period of October 1, 2017 through August 31, 2018, this contract was maintained and executed by QTS Realty Trust, Inc. (QTS). As of September 1, 2018, General Datatech, LP (GDT) assumed Kronos' contract previously held with QTS, becoming the managed service provider for the Workforce Ready

Partner Network product. GDT is responsible for maintaining the current service level and support as previously contracted between Kronos and QTS under the agreement. For all services, except for physical security, environmental safeguards, and antivirus management; Kronos Management maintains ownership and oversight of related controls.

Infrastructure

The infrastructure supporting the Workforce Ready Partner Network environment exists in a modular environment comprised of 'pods.' Each pod is bordered by redundant firewall technology, which is responsible for traffic policing and policy enforcement, both in and out of the pod. Users accessing the infrastructure (e.g. servers, databases) are authenticated and authorized through Active Directory membership, group policy enforcement, public key cryptography, and two-factor authentication methods. Each pod consists of multiple redundant application servers and multi-tenant Microsoft SQL Server databases. Customer specific configurations and data are segmented logically within the databases.

Software

The applicable software supporting the Workforce Ready Partner Network environment 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 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 and application systems in support of the Workforce Ready Partner Network 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. Data in transmissions are encrypted using Transport Layer Security (TLS) sessions. Data security is further discussed in the “Data Transmission” and “Availability” sections of this report. Access to Customer data in Workforce Ready Partner Network is limited to authorized Kronos personnel, and is granted in accordance with Kronos system security administration policies.

Application

The Workforce Ready Partner Network application is designed, deployed and maintained by Kronos resources to be delivered to Customers using the public internet. The Workforce Ready Partner Network application is a human capital management suite that is compiled from the following modules: Human Resources (HR), Payroll (PR), Time and Labor Management (TLM), Leave, Accruals, Compensation, Scheduler, Affordable Care Act (ACA), Talent Acquisition (TA), and Performance Management. The solutions can be utilized individually, as a complete suite, or in conjunction with other third-party applications, content and services. Customers have the flexibility to choose which modules they would like to purchase in order to meet the unique needs of their organization. The following table highlights module options by region:

Module	United States	Europe	Australia	Latin America
Time & Labor Management	X	X	X	X
Human Resources	X	X	X	X
Payroll	X			
Leave of Absence	X			
Accruals	X	X	X	X
Affordable Care Act (ACA)	X			
Compensation	X	X		
Scheduler	X	X	X	X
Performance Management	X	X	X	
Talent Acquisition	X	X	X	
Attestation	X			

Once a new contract is signed between Kronos and a Customer, the information is input to Kronos's order management system which integrates with the Workforce Ready Partner Network application to create the Customer's instance of Workforce Ready Partner Network. If an existing Customer wishes to enable additional features in the application, the Customer can do so at any time.

Once a Customer's environment is created, the Kronos Professional Services team will start the implementation project with the Customer. This includes setting up initial users and configuring the product to the Customer's requirements. The Workforce Ready Partner Network solution can be configured and customized to include specific reports and features that are required by the Customer's organization. Once the Customer is "live" with the solution, Kronos will only make changes to Customer environments at the Customer's request, and in the event the Customer is unable to complete the task themselves. As the application is highly customizable, any input, processing, and output field configurations are also determined by and the responsibility of the Customer. The underlying application code logic, which forms the basis of the results of calculations displayed by the application, is subject to the Kronos change management controls to facilitate complete and accurate calculations of data. Implementations and changes are documented and tracked using a ticketing system.

Subservice organizations complementary controls

Kronos utilizes QTS (subservice organization) to provide data center hosting services, consisting of physical security, environmental safeguards, and antivirus management; to support Workforce Ready Partner Network. Kronos has implemented various monitoring activities to monitor the described services provided by QTS through their vendor management process which confirms that contractual commitments are being met and effective controls exist over third-party services. As of September 1, 2018, GDT assumed Kronos' contract previously held with QTS, becoming the managed service provider for the Workforce Ready Partner Network product. GDT is responsible for maintaining the current service level and support as previously contracted between Kronos and QTS under the agreement.

It is expected that the sub-service organizations have implemented the following controls to support achievement of the associated criteria:

Criteria Reference	Expected Subservice Organization Controls
CC5.5	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
CC5.6, CC5.8, CC6.1	Antivirus solutions are installed, configured, and managed by appropriate personnel, including keeping the definitions up to date.

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 WFRPN application meets their requirements and notifying Kronos timely with any required changes or enhancements. (CC2.1)
- 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 ensure that access remains restricted to authorized and appropriate personnel. (CC5.1, CC5.2, and CC5.6)
- 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. (CC5.7 and C1.3)
- 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. (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. (CC3.2 and 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. (CC5.4 and C1.2)
- User entities are responsible for reviewing changes to their data to ensure that all changes are appropriate and authorized. (CC7.4 and C1.1)
- User entities are responsible for reviewing notifications from Kronos of changes to the WFRPN 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. (CC2.6)
- User entities are responsible for communicating any identified incidents impacting the security, availability or confidentiality of the system to Kronos on a timely basis. (CC 2.5)
- User entities are responsible for reviewing application audit trails and notifying Kronos of any discrepancies or unauthorized activity. (CC4.1)
- 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. (C1.7 and C1.8)
- User entities are responsible for maintaining servers supporting the time-clock systems and restricting access to authorized individuals. (CC5.5 and C1.3)