SOC 3 ® Report

Description of Kronos Incorporated's Workforce Ready Infrastructure and Application Services System relevant to Security, Availability and Confidentiality

For the Period October 1, 2018 to September 30, 2019

Table of Contents

Management's Assertion Regarding the Effectiveness of Its Controls Over the Kronos Incorporated's Workforce Ready Infrastructure and Application System System

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

- Identifying the *Workforce Ready Infrastructure and Application Services System* (System) and describing the boundaries of the System, which are presented in the section below titled *System Description of the Workforce Ready Infrastructure and Application 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 Workforce Ready Infrastructure and Application Services System*
- Identifying, designing, implementing, operating, and monitoring effective controls over the *Workforce Ready Infrastructure and Application 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 General Datatech, LP (GDT), Google Cloud Platform and Sendgrid (subservice organizations) to provide data center hosting services consisting of physical security, environmental safeguards and antivirus management and various services including hosting, cloud computing, and SMTP relay, respectively. 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 GDT, Google Cloud Platform and Sendgrid'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 GDT, Google Cloud Platform and Sendgrid. Our examination did not extend to the services provided by GDT, Google Cloud Platform and Sendgrid and we have not evaluated whether the controls management assumes have been implemented at GDT, Google Cloud Platform and Sendgrid have been implemented or whether such controls were suitably designed and operating effectively throughout the period October 1, 2018 to September 30, 2019.

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 October 1, 2018 to September 30, 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

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 Workforce Ready Infrastructure and Application Services System (Assertion), that Kronos Incorporated's controls over the Workforce Ready Infrastructure and Application Services System (System) were effective throughout the period October 1, 2018 to September 30, 2019, 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 Workforce Ready Infrastructure and Application Services 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 Workforce Ready Infrastructure and Application Services System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement.

Kronos uses General Datatech, LP (GDT), Google Cloud Platform and Sendgrid (subservice organizations) to provide data center hosting services consisting of physical security, environmental safeguards and antivirus management and various services including hosting, cloud computing, and SMTP relay, respectively. 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 GDT, Google Cloud Platform and Sendgrid'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 GDT, Google Cloud Platform and Sendgrid. Our examination did not extend to the services provided by GDT, Google Cloud Platform and Sendgrid and we have not evaluated whether the controls management assumes have been implemented at GDT, Google Cloud Platform and Sendgrid have been implemented or whether such controls were suitably designed and operating effectively throughout the period October 1, 2018 to September 30, 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

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

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

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 October 1, 2018 to September 30, 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 October 1, 2018 to September 30, 2019.

Ernst & Young LLP

December 6, 2019

System Description of the Workforce Ready 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 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

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 Infrastructure and Application Services supporting the production instances of Workforce Ready for customers in the United States (US), Australia (AU), and Europe (EU). Production instances are in third-party data center co-locations in Dulles, Virginia and Amsterdam, Netherlands (EU only). The scope of this description does not include the provisioning of Customer access to the Customer's instance of the application or any Customer self-customizations (i.e. input, processing or output field configurations) within their environment.

Region	Production data center location (managed by subservice organization)	Disaster recovery data center location (managed by subservice organization)
United States	Dulles, Virginia United States (GDT)	Phoenix, Arizona United States (GDT)
Europe	Amsterdam, Netherlands (GDT)	London, United Kingdom (GDT)
Australia	Dulles, Virginia United States (GDT)	Phoenix, Arizona United States (GDT)
Australia[1]	Sydney, Australia (Google)	N/A

[1] Customers based in Australia went live with the Google Cloud Platform on September 12, 2019. Google uses high availability technology within its regions. If a specific data center were to be unavailable, the Workforce Ready traffic automatically transfers to another Google Data Center within the region.

Product overview and service

The Workforce Ready (WFR) Infrastructure and Application Services 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 (PR), and time and labor management (TLM). 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 solution is offered to Kronos' customers (Customers) subscribing to one or more of the product's core modules. Workforce Ready is available any time, from anywhere through a front-end interface called Workforce Ready. Customers of Workforce Ready receive 24x7 access to their solution without having to purchase additional hardware, operating systems, or database licenses. Workforce Ready provides Customers with valuable peace of mind, knowing that experienced Kronos technical consultants are managing their applications and employee data. Workforce Ready 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, General Datatech (GDT), 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. For all services, except for physical security, environmental safeguards, and antivirus management; Kronos Management maintains ownership and oversight of related controls.

As of September 12, 2019, Australian customers hosted in the Google Public Cloud are bordered by redundant network firewalls, which are responsible for traffic policing and policy enforcement, both inbound and outbound traffic, and internal traffic. Users accessing the infrastructure (e.g. servers, databases) are authenticated and authorized through directory services via a privileged identity management (PIM) and/or SSL VPN tool with multi-factor authentication (MFA). Customer specific configurations and data are segmented logically within the database.

WFR leverages SendGrid as a service to provide SMTP relay to Customers; reports from Workforce Ready will leverage this service to send emails to customer users as well as internal alerting.

Components of the system

Infrastructure

The infrastructure supporting the Workforce Ready 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 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.

Application

The Workforce Ready application is designed, deployed and maintained by Kronos resources to be delivered to Customers using the public internet. The Workforce Ready application is a human capital management suite that is compiled from the modules in the table below:

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

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 to meet the unique needs of their organization.

Once a new contract is signed between Kronos and a Customer, the information is input to Kronos' order management system which integrates with the Workforce Ready application to create the Customer's instance of Workforce Ready. 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 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.

3.2.2.4 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. 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 [and application systems] in support of the Workforce Ready 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 Workforce Ready System 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 Vendor organizations as it relates to the Workforce Ready System:

- General Datatech (GDT): General Datatech provides data center hosting services, consisting of physical security, environmental safeguards, and antivirus management.
- Google Cloud: Google Cloud is utilized for computing and hosting services to store and maintain Workforce Ready customer data.
- SendGrid: SendGrid provides the SMTP relay that allows Kronos and Workforce Ready Customers to receive report content and alerts, if they are configured in various tools that support environment monitoring and backups.

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 GDT, Google and SendGrid through their vendor management process which confirms that contractual commitments are being met and effective controls exist over third-party services.

Subservice provider	Criteria reference	Expected subservice organizations controls
GDT Google Cloud	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.
GDT Google Cloud	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
GDT	CC6.8	Antivirus solutions are installed, configured, and managed by appropriate personnel, including keeping the definitions up to date.

Subservice provider	Criteria reference	Expected subservice organizations controls
Google Cloud	C1.2	Customer data that is uploaded or created is encrypted at rest.
Google Cloud	CC2.5 CC6.2	Google has an established incident response policy that outlines management responsibilities and procedures to help ensure a quick, effective, and orderly response to information security incidents.
Google Cloud	CC2.5, CC6.1	Google provides a process to internal users for reporting security, confidentiality and availability failures, incidents, and concerns, and other complaints.
Google Cloud	CC2.6, C1.6	System changes that may affect security, availability or confidentiality are communicated to management and users who will be affected.
Google Cloud	CC6.4	Annual data center security reviews are performed, and results are reviewed by executive management.
Google Cloud	CC5.7	Google does not permit equipment from leaving Google data centers without being subject to Google's sanitization process.
Google Cloud	CC6.1 C1.8	Encryption is used for traffic traversing fiber between Google production facilities.
Google Cloud	CC6.1, A1.1, A1.2	Redundant architecture exists such that resources are distributed across geographically dispersed data centers to support continuous availability.
SendGrid	A1.2	The SMTP server is monitored for availability to help ensure that Customer's emails are transmitted continuously, with respect to the WFR environment.
SendGrid	A1.2	SendGrid contracts with multiple data centers to permit the resumption of IT operations in the event of a disaster at its primary data center.
SendGrid	A1.2	Database backups are performed daily using an automated system.
SendGrid	A1.3	Information Security has documented a disaster recovery plan. This plan is tested at least annually, and test results are reviewed by plan stakeholders. If necessary, plan documentation is updated.

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 WFR application 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. (CC8.1)
- User entities are responsible for reviewing notifications from Kronos of changes to the WFR 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 application audit trails and notifying Kronos of any discrepancies or unauthorized activity. (C1.1)
- 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)