SOC 3 ® Report

Description of Kronos Incorporated's Workforce Dimensions HCM System relevant to Security, Availability, Confidentiality and Processing Integrity

For the Period May 1, 2018 to October 31, 2018

Table of Contents

Management's Assertion Regarding the Effectiveness of Its Controls Over the Kronos Incorporated's Workforce Dimensions HCM System Based on the Trust Services Principles and Criteria for Security, Availability, Confidentiality and Processing Integrity

Kronos utilizes the Google Cloud Platform and SendGrid (subservice organizations) to provide various services including hosting, cloud computing and SMTP relay. The Description includes only the control objectives and related controls of Kronos and excludes the control objectives and related controls of the subservice organizations. The Description also indicates that certain control objectives specified in the Description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The Description does not extend to controls of the subservice organization.

We, as management of Kronos, are responsible for designing, implementing and maintaining effective controls over the Kronos Incorporated's Workforce Dimensions HCM 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 May 1, 2018 to October 31, 2018, to achieve the commitments and system requirements related to the operation of the System using the criteria for security, availability, confidentiality, and processing integrity (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 May 1, 2018 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
- the System processing is complete, valid, accurate, timely, and authorized 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 Kronos Incorporated's Workforce Dimensions HCM System identifies the aspects of the Kronos Incorporated's Workforce Dimensions HCM System covered by our assertion.

The Management of Kronos Incorporated
December 14, 2018

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 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 Dimensions HCM System was protected against unauthorized access, use, or modification to achieve Kronos' commitments and system requirements;
- the Workforce Dimensions HCM System was available for operation and use to achieve Kronos' commitments and system requirements; and
- the Workforce Dimensions HCM System information is collected, used, disclosed, and retained to achieve Kronos' commitments and system requirements
- the Workforce Dimensions HCM System processing is complete, valid, accurate, timely, and authorized to achieve Kronos' commitments and system requirements

during the period May 1, 2018 to October 31, 2018 based on the criteria for security, availability, confidentiality, and processing integrity 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, processing integrity and confidentiality are achieved.

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

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

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

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, processing integrity and confidentiality.

Ernst & Young LLP

December 14, 2018

System Description of the Workforce Dimensions HCM 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 Dimensions HCM System (hereafter referred to as Workforce Dimensions or WFD) is comprised of Infrastructure and Application Services that provides Software as a Service (SaaS) based workforce management applications with a major focus in delivering solutions that support timekeeping, scheduling, leave and attendance, human resources, and payroll. Kronos delivers the platform for applications and third-party offerings to be accessed within one interface. The Workforce Dimensions solution is hosted on the Google Cloud Platform (hereafter referred to as GCP) providing Customers with the benefit of high availability within the public cloud. WFD leverages SendGrid as a service to provide SMTP relay to customers; reports from Workforce Dimensions will leverage this service to send emails to customer users, as well as internal alerting. Workforce Dimensions is available any time, from anywhere through two front-end interfaces called Workforce Dimensions and HCM. Workforce Dimensions provides customers access into the time and attendance components of the solution (hereafter referred to as core Workforce Dimensions) and HCM complements this to provide access to the HR and Payroll modules. Customers of Workforce Dimensions receive 24x7 access to their solution without having to purchase additional hardware, operating systems, or database licenses.

Infrastructure

The infrastructure supporting the Workforce Dimensions environment exists in the GCP, who use the concepts of regions and zones. A region is a specific geographical location where Customers can run the environment and is comprised of one or more zones. For example, the us-central1 region denotes a region in the Central United States that has zones us-central1-a, us-central1-b, us-central1-c, and us-central1-f. Workforce Dimensions resides in multiple zones. Data is shared among the data centers within a region to provide redundancy and high availability within the region. All customer data resides within the

Workforce Dimensions environment located in GCP, either in US East and US Central, North America Northeast, or Australia Southeast depending on the origin of the customer. HCM functionality is only available in the US East and US Central geographies. This ecosystem is bordered by redundant L3 and L7 firewall technologies, which are responsible for traffic policing and policy enforcement, both in and out of the environment 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.

Software

The applicable software supporting the Workforce Dimensions 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, automated deployment management, ingress and server virus protection, and vulnerability management. Access to and use of these utilities is restricted to 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 Dimensions 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 or Secure File Transmission Protocol (SFTP). Access to customer data in Workforce Dimensions is limited to authorized Kronos personnel, and is granted in accordance with Kronos system security administration policies.

Application

The Workforce Dimensions application is designed, deployed and maintained by Kronos resources to be delivered to Customers using the public internet. The Workforce Dimensions application is a workforce management suite with functionality for timekeeping, scheduling, leave and attendance, HR and payroll. Dell Boomi is a tool utilized for the integration between the Workforce Dimensions (WFD) application and customer third-party systems. The Dell Boomi tool manages key APIs within the WFD ecosystem as well as the APIs with external client environments. The solution comes with Dell Boomi accounts that allow Customers to create and deploy APIs to enable Workforce Dimensions to work seamlessly with other third-party applications.

Module	United States	Australia	Canada
Timekeeping	X	X	X
Scheduling	X	X	X
Leave & Attendance	X	X	X
HR	X		
Payroll	X		

Once a new contract is signed between Kronos and a Customer, Hosting Operations creates two new core Workforce Dimensions tenants for the Customer, a production and a non-production tenant, as well as one HCM tenant for HR and payroll functionality. The non-production tenant comes equipped with

baseline configurations designed for the vertical of the Customer. Customers can then log into their tenant and customize the configurations to meet their business requirements.

Kronos will only make changes to Customer environments at the Customer's request, 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 are 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 the following subservice organizations as it relates to the Workforce Dimensions system:

- **Google Cloud:** Google Cloud is utilized for computing and hosting services to store and maintain Workforce Dimension customer data.

- **SendGrid:** SendGrid provides the SMTP relay that allows Kronos and Workforce Dimensions customers to receive report content and alerts, if they are configured in various tools that support environment monitoring and backups.

Kronos has implemented various monitoring activities to monitor the services provided by Google and SendGrid 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 control objectives:

Subservice Provider	Criteria Reference	Expected Subservice Organization 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 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, processing integrity, and availability failures, incidents, and concerns, and other complaints.
Google Cloud	CC2.6, C1.6	System changes that may affect security, availability, processing integrity, or confidentiality are communicated to management and users who will be affected
Google Cloud	CC5.5	Annual data center security reviews are performed and results are reviewed by executive management.
Google Cloud	CC5.5	Physical security measures in place include: • Existence of security guards, access badges, and video cameras to secure the data centers is reviewed during the annual data center security reviews. • Data center entrances have a perimeter security system consisting of badge readers or biometric access system. • Data centers utilize badge reader or biometric access controls to restrict access to raised floor spaces and lock/keys to restrict access to facilities rooms within the building. • All emergency exit points from the raised floor are alarmed. • Badge reader and biometric control systems are secured in a restricted space and no physical access to them from public spaces exists. • Visitors to the datacenter facilities must gain approval, sign in at the front, and remain with an escort during the duration of their visit. • Video cameras exist to monitor building entrances, exists, and the areas immediately surrounding the building.

Subservice Provider	Criteria Reference	Expected Subservice Organization Controls
		• At least one security guard is on-site 24x7. • All staff members are required to either sign in or badge in to gain access to the facility and a no tailgating policy is in place. • All Google cages, suites, ad private rooms are secured using either lock/key, badge access control, or biometric access controls. A key sign out sheet and/or log of badge reader activity exists and covers access to Google spaces.
Google Cloud	CC5.5	Visitors must be signed in by an employee before a single-day paper visitor badge that authorizes them can be issued.
Google Cloud	CC5.5	All visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.
Google Cloud	CC5.5	User access lists to data center server areas are reviewed on a quarterly basis and inappropriate access is removed in a timely manner.
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, PI1.4, PI1.5, PI1.6	Redundant architecture exists such that resources are distributed across geographically dispersed data centers to support continuous availability.
Google Cloud	A1.2	All data centers are equipped with fire detection alarms and protection equipment. Data center server floors and network rooms are connected to a UPS system and emergency generator power is available in the event of a loss of power. Google protects the information system from damage resulting from water leakage by providing shutoff valves that are accessible, working properly and known to key personnel.
SendGrid	A1.2	The SMTP server is monitored for availability to help ensure that customer's emails are transmitted continuously, with respect to the WFD 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 Workforce Dimensions 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, CC5.6, and PI1.6).
- User entities are responsible for managing Kronos access to their tenants via the support profile (CC5.1, CC5.2, and CC5.6).
- User entities are responsible for communicating security, availability, processing integrity 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 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 WFD 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, confidentiality, or processing integrity 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 approving and validating the appropriateness (and maintaining the confidentiality) of data provided to Kronos and any changes to that data (C1.8).

- 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).

- User entities are responsible for determining that the transaction processing functionality within the Workforce Dimensions application meets their expectations and notifying Kronos timely with any required changes or enhancements (PI1.3 and PI1.5).

- User entities are responsible for the completeness and accuracy of data input to the Workforce Dimensions application via either direct data input or API (PI1.2).

- User entities are responsible for reviewing system outputs for completeness and accuracy and notifying Kronos of any discrepancies (PI1.5).

- User entities are responsible for monitoring all required scheduled jobs for timeliness and completeness and notifying Kronos if support is required (PI1.5).

- User entities are responsible for reviewing all configurations and APIs are part of their testing prior to providing the UAT signoff in the implementation process (PI1.2, PI1.5 and CC7.1).

- User entities are responsible for ensuring that changes to APIs, including any configurations, are authorized, tested and approved (PI1.1, PI1.3, PI1.4, and PI1.5).