SOC 3 ® Report

Description of UKG Incorporated's UKG HR Service Delivery (UKG HRSD) System and Services relevant to Security, Availability, Confidentiality, and Privacy

For the Period October 1, 2021 to September 30, 2022

Table of Contents

Management's Report of its Assertions on the Effectiveness of Its Controls over the UKG HR Service Delivery (UKG HRSD) Based on the Trust Services Criteria for Security, Availability, Confidentiality and Privacy

February 3, 2023

We, as management of, UKG Incorporated (UKG or Service Organization) are responsible for:

- Identifying the UKG HR Service Delivery (UKG HRSD) (System) and describing the boundaries of the System, which are presented in the section below titled *System Description of the UKG HR Service Delivery System*
- Identifying our principal service commitments and system requirement
- 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 UKG HR Service Delivery System*
- identifying, designing, implementing, operating, and monitoring effective controls over the UKG HR Service Delivery (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

UKG uses Rackspace, Eucrites and AWS to provide data center hosting services. Additionally, UKG uses Mandiant to provide endpoint detection services. Collectively, these external subservice organizations are referred to as the subservice organizations. The Description of the boundaries of the System indicates that UKG's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if the subservice organizations' controls, assumed in the design of UKG's controls, are suitably designed and operating effectively along with related controls at the service organization. The Description includes only the controls of UKG and excludes controls of the subservice organizations, however it does present the types of controls that UKG assumes have been implemented, suitably designed, and operating effectively at the subservice organizations. The Description also indicates that certain trust services criteria specified therein can be only met if the subservice organizations' controls assumed in the design of UKG's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of the subservice organizations.

However, we perform annual due diligence procedures for third-party subservice providers and based on the procedures performed, nothing has been identified that prevents UKG from achieving its specified service commitments.

We assert that the controls over the system were effective throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, confidentiality and privacy set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

The Management of UKG Incorporated

Ernst & Young LLP
Suite 500
5100 Town Center Circle
Boca Raton, FL 33486

Tel: +1 561 955 8000
Fax: +1 561 955 8200
ey.com

Report of Independent Accountants

To the Board of Directors
UKG Incorporated

Scope
We have examined management's assertion, contained within the accompanying *Management's Report of its Assertions on the Effectiveness of Its Controls over the UKG HR Service Delivery (UKG HRSD)* (Assertion), that UKG Incorporated's controls over the UKG HR Service Delivery (System) were effective throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, confidentiality and privacy (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
UKG's management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the UKG HR Delivery Service (System) and describing the boundaries of the System
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of the system
- Identifying, designing, implementing, operating, and monitoring effective controls over the UKG HR Delivery Service (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement

UKG uses Rackspace, eucrites and AWS to provide data center hosting services. Additionally, UKG uses Mandiant to provide endpoint detection services. Collectively, these external subservice organizations are referred to as the subservice organizations. The Description of the boundaries of the System indicates that UKG's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if the subservice organizations' controls, assumed in the design of UKG's controls, are suitably designed and operating effectively along with related controls at the service organization. The Description includes only the controls of UKG and exclude controls of the subservice organizations, however it does present the types of controls that UKG assumes have been implemented, suitably designed, and operating effectively at the subservice organizations. Our examination did not extend to the services provided by the subservice organizations and we have not evaluated whether the controls management assumes have been implemented at the subservice organizations have been implemented or whether such controls were suitably designed and operating effectively throughout the period October 1, 2021 to September 30, 2022.

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 ("AICPA"). 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 UKG's relevant security, availability, confidentiality and privacy 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 UKG's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

We are required to be independent of UKG and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

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 UKG's 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, UKG's controls over the system were effective throughout the period October 1, 2021 to September 30, 2022, 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 UKG's controls throughout the period October 1, 2021 to September 30, 2022

Restricted use
This report is intended solely for the information and use of UKG and prospective customers of UKG HR Service Delivery and is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst & Young LLP

February 3, 2023

System Description of the UKG HR Service Delivery (HRSD) System

Overview of the organization and services

Ultimate Kronos Group (UKG) is a global privately held company, serving organizations in more than 100 countries, including many Fortune 1000 companies. The company is built on 70 years of experience from two leaders in Human Resources (HR) solutions, combining the strength and innovation of Ultimate Software and Kronos Incorporated. Customers use UKG solutions in areas such as:

Human Capital Solutions

- Human Resources
- Hiring
- Benefits Administration
- Training & Development

Workforce Management Solutions

- Time and Attendance
- Scheduling
- Absence Management
- Payroll & Tax Filing
- Labor Analytics
- Document Management

UKG's human capital and workforce management solutions provide the complete automation and high-quality information Customers require to help manage labor costs, minimize compliance risk and improve workforce productivity.

UKG's technology helps reduce the complexities involved with the ongoing maintenance of a business system. UKG provides comprehensive hosting, maintenance and support of its Human Capital Management (HCM) workforce management, and other solutions, including complete support of IT infrastructure encompassing computer hardware, operating systems, and database systems required to run UKG applications.

Scope of the report and overview of the services

This Description was prepared in accordance with the criteria set forth for a SOC 3® Type 2 Report in the Assertion of UKG Incorporated and the guidance for a description of a service organization's system set forth by the AICPA Attestation Standards.

The scope of the Description covers UKG's processes and controls relevant to the design, operation and maintenance of the infrastructure and application services supporting the production instances of UKG HR Service Delivery (HRSD), namely UKG People Assist (including Digital Process Manager), UKG Document Manager, UKG Employee Vault and UKG HRSD Advanced Analytics.

The scope of the Description does not include the platform's implementation process and the provisioning of Customer access to the Customer's web application.

Product overview and service

The UKG HRSD platform allows Human Resources (HR) teams to quickly answer employee requests on demand, automate employee processes, collect and understand employee feedback while remaining compliant across locations.

UKG HRSD's unique technology stack provides global organizations the ability to scale operational efficiency. The core components of the HRSD platform are UKG People Assist and UKG Document Manager, which form the foundation upon which additional modules can be added: Digital Process Manager (Process Automation), UKG Employee Vault (for EU customers only) and UKG HRSD Advanced Analytics:

- **UKG People Assist**
  - Digital Process Manager (Process Automation)

- **UKG Document Manager**
  - UKG Employee Vault (for EU customers only)
  - UKG HRSD Advanced Analytics

UKG People Assist empowers employees to find personalized HR information via an employee knowledge base and enables HR to route and rapidly respond to more complex, non-routine requests.

Digital Process Manager (Process Automation) creates global processes that are personalized based on employee attributes to support local exceptions.

UKG Document Manager, also called Employee File Management, allows HR to actively manage documents efficiently and compliantly: create, sign, store, access, share and delete employee files in one secure place, accessible on any device and available wherever the clients are.

The Employee Vault allows clients to distribute any type of document directly to the employees, which enables them to manage all their employment documents from within a private and secure account. The Employee Vault is integrated with UKG Document Manager, allowing clients to securely store and actively manage the entire employee file life cycle (from document creation to expiration).

UKG HRSD Advanced Analytics arms clients to prioritize resources and actions for maximum impact, to spot bottlenecks and track performance to proactively deliver the best possible employee support, relevant insights and timely feeds of information.

Components of the system

Infrastructure

Clients can choose the geography of the platform from which the HRSD services will be delivered. The technical infrastructure is hosted by Infrastructure as a Service (IaaS) service providers located in the following locations:

HRSD platform	Technical infrastructure is hosted by:	Services provided	Hosting location
Europe	Rackspace for documents for clients' model data	• Network infrastructure • Physical computing resources • Hardware maintenance and update	Frankfurt, Germany
	Ecritel for clients' data documents	• Network infrastructure • Physical computing resources • Data replication	Paris, France
United States	Rackspace	• Network infrastructure • Physical computing resources • Data replication • Hardware maintenance and update	Texas, United States (Primary) Virginia, United States (Secondary)

Rackspace is a global provider in IaaS services and provides its clients with both SOC 2 reports and ISO/IEC 27001 certification. Ecritel is a French hosting management company that provides its services under a SOC 2 report and ISO/IEC 9001 certification. Ecritel hosts its infrastructures in data centers managed by Equinix and Global Switch, which provide their services under ISO/IEC 27001 certification.

Amazon Web Services (AWS) provides services for the off-site backup storage.

UKG Pro North American clients can also use the UKG HRSD system as part of the UKG Pro Full Suite. For those clients, the technical infrastructure is hosted by IaaS providers located in the following locations:

HRSD platform	Technical infrastructure is hosted by:	Hosting location
Canada	Cyxtera Technologies Inc.	Toronto, Canada
United States Atlanta	Quality Technology Services Inc. (QTS)	Atlanta, United States (Primary)
	Switch Ltd.	Las Vegas, United States (Secondary)

Software

The software supporting the relevant UKG products and services includes various utilities that are used by UKG personnel in managing and monitoring the environment. These utilities are used in control processes including, but not limited to, high availability and redundancy, backups and replication, patch management, cloud automation and deployment, performance and security monitoring, antivirus and antimalware management, automation testing, and database management. Access to and use of these utilities is restricted to appropriate personnel who require such access to complete their job responsibilities.

Application

The UKG HRSD platform is a Software as a Service (SaaS) multi-tenant platform designed, deployed and maintained by UKG resources to be delivered to Customers using the public internet. Three instances of the platform can be chosen from by Customers: European Union, United States or Canada.

Data

Customer data is held in accordance with applicable data protection and other regulations set out in customer contracts. Access to electronically held customer data is granted only to authorized personnel using the principle of least privilege. Customer data at rest is housed in a database management system managed by the UKG HRSD Database team. Data in transit is encrypted using various methods as applicable, such as Transport Layer Security (TLS) sessions and Secure File Transmission Protocol (SFTP).

Procedures

UKG has documented policies and procedures to support the operations and controls over its relevant products and services. Relevant policies and procedures are made available to employees through the corporate intranet sites.

Service commitments and system requirements

UKG designs its processes and procedures relevant to the System to meet objectives of applicable services. UKG's objectives are based on the service commitments made to the Customers in relevant contracts, applicable laws, and regulations.

UKG establishes operational requirements that support the achievement of its applicable security, availability, processing integrity, confidentiality, and privacy commitments; relevant laws and regulations; and other system requirements. Such requirements are communicated in UKG's policies and procedures, system design documentation and contracts with third parties (Customers and vendors). The principal service commitments and system requirements commitments include:

- 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 UKG' processes over protecting data and promote staff awareness of data protection processes.
- Implementing logical access restrictions to help ensure that logical 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.
- Executing a vendor risk management process to include oversight and contractual commitments from third parties that are consistent with UKG's expectations.
- Processing of transactions in accordance with the system documentation and requirements.
- Inventorying data in a way to achieve accurate reporting of processing activities conducted on behalf of Customers.
- As a data processor, assessing privacy and risk continuously, including General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), other local privacy regulations,

and contractual requirements, as applicable, as UKG products and processes evolve, utilizing the Data Inventory and Classification methodology outlined in UKG policy.
- Providing mechanisms and/or information to allow Customers to obtain data subject consent and communicate their data collection processes.

Subservice organizations complementary controls

Carved-out unaffiliated subservice organizations

Applicable to Customers using the Europe platform and the US platform to utilize HRSD services.

UKG utilizes the following subservice organizations as they relate to the HRSD System:

- **Rackspace:** provides network infrastructure, physical computing resources, data replication and hardware maintenance and update services.
- **Ecritel**: provides network infrastructure, physical computing resources, and data replication.
- **Amazon Web Services (AWS):** provides services for the off-site backup storage.
- **Mandiant:** provides endpoint detection services

UKG has implemented various monitoring activities to monitor the services provided by the subservice organizations noted above 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 trust service criteria:

Types of controls expected to be implemented at the subservice organization	Applicable Trust Service Criteria	Applicable subservice organizations
UKG expects that the subservice organizations have implemented controls for restricting logical access to their environments.	CC6.1, CC6.2, CC6.3	Rackspace Ecritel AWS
UKG expects that the subservice organizations have implemented controls for restricting physical access to the data centers to authorized and appropriate personnel for their applications and services.	CC6.4	Rackspace Ecritel AWS
UKG expects that the subservice organizations have implemented controls for disposing of and removing the ability to read or recover data and software from decommissioned hardware assets.	CC6.5	Rackspace Ecritel AWS
UKG expects that the subservice organizations have implemented controls for maintaining security measures to protect against threats from sources outside the system.	CC6.6	Rackspace Ecritel AWS
UKG expects that the subservice organizations have implemented controls to help ensure data is restricted and protected during transmission, movement, and removal.	CC6.7	Rackspace Ecritel AWS

Types of controls expected to be implemented at the subservice organization	Applicable Trust Service Criteria	Applicable subservice organizations
UKG expects that the subservice organizations have implemented controls for maintaining security measures to protect against the introduction of unauthorized or malicious software.	CC6.8	Rackspace Ecritel AWS
UKG expects that the subservice organizations have implemented controls for maintaining application and system processing to their applications and services.	CC7.2, CC8.1	Rackspace Ecritel AWS
UKG expects that the subservice organizations have implemented controls for identifying and reporting incidents to appropriate personnel and acting on accordance with established incident response procedures.	CC7.2, CC7.3	Rackspace Ecritel AWS Mandiant
UKG expects that the subservice organizations have controls for valid, complete, accurate and timely changes to the network infrastructure supporting their applications and services.	CC8.1	Rackspace Ecritel AWS
UKG expects that the subservice organizations have implemented controls for maintaining and monitoring current processing capacity and usage.	A1.1	Rackspace Ecritel AWS
UKG expects that the subservice organizations have implemented control for environmental protections to the data centers.	A1.2	Rackspace Ecritel AWS
UKG expects that the subservice organizations have implemented controls for maintaining and testing business continuity and disaster recovery plans.	A1.3	Rackspace Ecritel AWS

User entity responsibilities

While there are no complementary user entity controls, user entities are responsible for the configuration of the security of their own environment. These responsibilities include, but are not limited to:

- User entities are responsible for implementation, enforcement and monitoring of Customer business rules applicable to their use of the system, including Customer and Customer employee provided files and data.
- User entities are responsible for the user access management (creation, modification, and deletion) for their own employees and third parties.
- User entities are responsible for configuration of complex or strong passwords and multi-factor authentication for use when authenticating and managing them for continued appropriateness. Implementations and maintenance of secure password reset procedures, including standards for complex or strong default passwords.
- User entities are responsible for enabling and configuring session timeout security settings and Internet Protocol (IP) address filters for login.
- User entities are responsible for reporting any security-, availability- and confidentiality-related issues to the Customer Support team in a timely manner. User entities are responsible for monitoring for and responding to the Customer Support team on actions required to support issue resolution.

- User entities are responsible for identifying and communicating users who have the authority to communicate requests for account decommissioning and other changes to terms of service.
- User entities are responsible for notifying UKG to delete their data following contract termination.
- User entities are responsible for providing data subjects notice of company practices designed to meet the entity's objective related to privacy. Updates and changes made to the notice are communicated to data subjects in a timely manner.
- User entities are responsible for implementing controls that obtain consent from their data subjects prior to the collection of their personal information, communicating the need for such consent, and communicating consequences of failure to provide consent.
- User entities are responsible for reading provided documentation related to UKG suppliers and notifying UKG with any concerns and/or changes with these suppliers.
- User entities are responsible for providing physical and electronic copies of personal information upon the data subject's request. Denial to provide such information will be communicated to the data subject by the entity.