SOC 3 ® Report

Description of UKG Incorporated's UKG Private Cloud Infrastructure Services System relevant to Security, Availability, Confidentiality, and Privacy

For the Period March 1, 2022 to October 31, 2022

Table of Contents

Management's Report of its Assertions on the Effectiveness of its Controls over UKG Incorporated's UKG Private Cloud Infrastructure Services System Based on the Trust Services Criteria for Security, Availability, Confidentiality, and Privacy

December 22, 2022

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

- Identifying the *UKG Private Cloud Infrastructure Services System* (System) and describing the boundaries of the System, which are presented in the section below titled *System Description of the UKG Private Cloud Infrastructure 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 UKG Private Cloud Infrastructure Services System*
- Identifying, designing, implementing, operating, and monitoring effective controls over the *UKG Private Cloud Infrastructure 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

UKG uses Cyxtera Technologies, Inc. (Cyxtera) and Equinix, Inc. (Equinix), external subservice organizations, to provide various services, including data center hosting services, physical security, and environmental controls. Additionally, UKG uses Mandiant, an external subservice organization, to provide endpoint detection services. Collectively, these external subservice organization 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 March 1, 2022 to October 31, 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 of the Effectiveness of Its Controls over UKG Incorporated's UKG Private Cloud Infrastructure Services System* (Assertion), that UKG Incorporated's (UKG) controls over the UKG *Private Cloud Infrastructure Services System* (System) were effective throughout the period March 1, 2022 to October 31, 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 Private Cloud Infrastructure Services System (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 its principal service commitments and service requirements that are the objectives of our system
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirements.

UKG uses Cyxtera Technologies, Inc. (Cyxtera) and Equinix, Inc. (Equinix), external subservice organizations, to provide various services, including data center hosting services, physical security, and environmental controls. 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. 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 March 1, 2022 to October 31, 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 March 1, 2022 to October 31, 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 March 1, 2022 to October 31, 2022.

Restricted Use
This report is intended solely for the information and use of UKG and current and prospective customers of the UKG Private Cloud Infrastructure Services system and is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst & Young LLP

December 22, 2022

System Description of the UKG Private Cloud Infrastructure Services System

Overview of the organization and services

UKG Incorporated (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 manage labor costs, minimize compliance risk, and improve workforce productivity.

UKG's technology helps eliminate the complexities involved with the ongoing maintenance of a business system. UKG provides comprehensive hosting, maintenance, and support of the Human Capital Management (HCM) solution, 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 2® Type 2 Report in the Assertion of UKG Incorporated 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 UKG's processes and controls relevant to the design, operation and maintenance of the UKG Private Cloud Infrastructure Services System (hereafter referred to as Private Cloud) at the following locations:

- Waltham, Massachusetts
- Chicago, Illinois
- Frankfurt, Germany
- Amsterdam, Netherlands

The scope of the Description does not include the application layer (including application end-user authentication) of Customer systems, as Customers are responsible for managing these technology components and thus are not considered part of the UKG Private Cloud Infrastructure Services System. This description only pertains to infrastructure components such as the network, operating system, database layers, and Citrix.

Product overview and service

UKG's Private Cloud hosts and manages the infrastructure components of UKG workforce management solutions, where Customers can access their application(s) over the Web at any time, from anywhere through the front-end interfaces. Private Cloud Customers receive 24x7 access to their solution without having to purchase additional hardware, operating systems, or database licenses. Private Cloud services provide Customers with experienced UKG technical consultants which help support the infrastructure hosting their applications and employee data. Private Cloud is an ideal choice for organizations seeking to achieve their workforce management goals without exceeding their capital equipment budgets or placing additional demands on their in-house Information Technology (IT) staff.

Components of the system

Infrastructure

The infrastructure supporting the Private Cloud environment is segmented into modular environments referred to as 'pods.' Each pod is bordered by redundant firewall technology, provided by two different vendors, which is responsible for traffic policing and policy enforcement both inbound and outbound of the pod, as well as within Layer 2 & 3 network controls. Individual Customer and infrastructure servers, which run on Windows Server operating systems, are authenticated/authorized through Active Directory membership, group policy enforcement, privileged access management, multi-factor authentication, and public key cryptography. Customer specific configurations and data are maintained on Microsoft SQL databases (which are also subject to Active Directory controls, group policy enforcement, and privileged access management) and are isolated on a per Customer, per network basis. To support inbound and outbound transmissions, the Private Cloud environment also contains a 'file transfer manager' that uses Secure File Transfer Protocol (SFTP). In addition, Customer access to infrastructure resources is authenticated and authorized through the Citrix accounts.

UKG is contracted with industry recognized data center providers that provide data center space, power, and connectivity for the infrastructure supporting the Private Cloud environment.

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.

Data

Customer data is held in accordance with applicable data protection and other regulations set out in Customer contracts and UKG policies and procedures. Access to electronically held Customer data is granted only to authorized personnel using the principle of least privilege. Customer data at rest is securely housed in a database management system, while data in transit is encrypted over secure channels.

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 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, 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:

- 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.
- 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's processes over protecting data and promote staff awareness of data protection processes.
- Executing a vendor risk management process to include oversight and contractual commitments from third parties that are consistent with UKG 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), and other local privacy regulations, as applicable, and contractual requirements, as UKG products and processes evolve, utilizing the Data Inventory and Classification system.
- Providing mechanisms and/or information to allow Customers to obtain data subject consent or communicate their data collection processes.

Subservice organizations complementary controls

Carved-out unaffiliated subservice organizations

UKG utilizes the following subservice organizations as they relate to the Private Cloud Infrastructure Services System:

- **Cyxtera:** Cyxtera provides data center hosting services, including physical security and environmental safeguards.
- **Equinix:** Equinix provides data center hosting services, including physical security and environmental safeguards.
- **Mandiant:** Mandiant provides endpoint detection and response services.

UKG has implemented various monitoring activities to monitor the services provided by the subservice organizations noted above through its vendor management program, 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.

Subservice organization(s)	**Criteria**	**Expected subservice organization controls**
Cyxtera Equinix	CC2.2 CC2.3	Controls to address system changes that may affect security, privacy, or confidentiality are communicated to management and users who are affected.
Mandiant	CC2.2 CC7.2	Controls to address a process for internal users to report security, confidentiality, and privacy failures, incidents, and concerns, and other complaints.
Cyxtera Equinix Mandiant	CC2.2 CC7.3 P6.3 P6.4 P6.5 P6.6	Controls to notify UKG of any incidents or breaches.
Cyxtera Equinix	CC6.4	Controls to address physical access and environmental protections to computer equipment and storage media are established.
Cyxtera Equinix	A1.1 A1.2 A1.3	Controls to address the entity's ability to maintain continuous operations and react to availability incidents are in place.

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 reviewing relevant audit trails and notifying UKG of any discrepancies or unauthorized activity.
- 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.
- User entities are responsible for determining that the functionality within the UKG system meets their requirements and notifying UKG timely with any required changes or enhancements.
- User entities are responsible for ensuring their systems are in compliance with regulatory requirements and state laws, any specific requirements should be communicated to UKG in a timely manner.
- 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.
- User entities are responsible for ensuring information shared as part of the implementation scoping is accurate in order to meet system funcitionality requirements of the business.
- User entities are responsible for designating appropriate individuals in their respective organizations to authorize and approve requests for new and modified access to the user entities data available through Private Cloud.
- User entities are responsible for reviewing access to their environment and notifying UKG of any discrepancies.
- User entities are responsible for managing application access (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.
- User entities are responsible for ensuring that each user is assigned a unique login and for taking necessary steps to safeguard passwords and user credentials.
- User entities are responsible for approving and validating the appropriateness (and maintaining the confidentiality) of data provided to UKG and any changes to that data.
- User entities are responsible for maintaining servers supporting the time-clock systems and restricting access to authorized individuals.
- User entities are responsible for adequately securing and disposing of any system output.
- User entities are responsible for appropriately securing transmissions of data to UKG, which includes transmissions from middleware, and informing UKG of any necessary changes to the System.
- User entities are responsible for communicating any identified incidents impacting the security, availability, or confidentiality of the system to UKG on a timely basis.
- User entities are responsible for reviewing notifications from UKG of changes to the Private Cloud environment and communicating any concerns to UKG.
- User entities are responsible for reviewing changes to their data to help ensure that all changes are appropriate and authorized.
- User entities are responsible for communicating any changes to their data retention and destruction requirements from the original contract terms to UKG in a timely manner.
- 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 reading provided documentation related to UKG suppliers and notifying UKG with any concerns and/or changes with these suppliers.

- 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 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.