SOC 3 ® Report

Description of UKG Incorporated's UKG Payroll Services System relevant to Security, Availability, and Confidentiality

For the Period March 1, 2022 to September 30, 2022

Table of Contents

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

December 21, 2022

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

- Identifying the UKG Payroll Services System (System) and describing the boundaries of the System, which are presented in the section below titled *System Description of the UKG Payroll 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 Payroll Services System*
- Identifying, designing, implementing, operating, and monitoring effective controls over the *UKG Payroll Services System* (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion

UKG uses Cyxtera Technologies, Inc. (Cyxtera) and Mandiant, external subservice organizations, to provide hosting services, including physical security and environmental safeguards and endpoint detection services, respectively. 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, 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, and confidentiality 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 Payroll Services System* (Assertion), that UKG Incorporated's (UKG) controls over the UKG Payroll Services System (System) were effective throughout the period March 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, 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
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 Payroll 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 System to mitigate risks that threaten the achievement of the principal service commitments and system requirements.

UKG uses Cyxtera Technologies, Inc. (Cyxtera) and Mandiant, external subservice organizations, to provide hosting services, including physical security and environmental safeguards, and endpoint detection services, respectively. Collectively, Cyxtera and Mandiant 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 organizations. 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, 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 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 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, 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 March 1, 2021 to September 30, 2022.

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

Ernst & Young LLP

December 21, 2022

System Description of the UKG Payroll 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 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 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 Payroll Services (UKGPS) System, including payroll distribution services, tax processing services, and the applicable supporting information technology (IT) general control environment and related IT processes managed by UKG. This includes the UKG Private Cloud environment in Waltham, Massachusetts and Chicago, Illinois; as well as the print production facilities located in Louisville, Kentucky; Irvine, California; and Memphis, Tennessee.

The scope of the Description does not include payroll processing services, which is performed by the UKG Dimensions and UKG Ready Human Capital Management (HCM) systems.

Product overview and service

The UKG Payroll Services (UKGPS) system is a provider of payroll distribution and tax processing services, for Customers using UKG Dimensions or UKG Ready as their HCM solution. Services include distributing employee checks and direct deposits, distributing vendor / garnishment checks and Automated Clearing House (ACH) payments, and preparing, filing, and paying payroll taxes for many tax jurisdictions.

UKGPS leverages several technology solutions, including the UKG Dimensions and UKG Ready applications (Payroll Systems) and multiple third-party applications to perform these services. UKGPS Customers are provided access to either Payroll System (depending on which the Customer purchased), whereas the third-party applications are used internally by UKGPS personnel to provide the services and facilitate execution of certain processes and controls described within this report.

Components of the system

Infrastructure

The infrastructure supporting the environment (consisting of the UKGPS Active Directory network, file shares, and its supporting Microsoft SQL Server database) is housed in a modular environment called a 'pod' within the UKG Private Cloud (Private Cloud). The UKGPS pod is bordered by redundant firewall technology, which is responsible for traffic policing and policy enforcement both in and out of the pod, as well as within Layer 2 & 3 network controls. 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.

UKG is contracted with an industry recognized data center provider, that provides 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.

Application

UKGPS uses several applications to support its payroll distribution and tax processing services:

- **Payroll Systems (UKG Dimensions and UKG Ready)**: The Payroll Systems are applications provided by the internal subservice organization, UKG Incorporated, and are hosted in the Google Cloud Platform. The controls around the hosting and development of these applications and underlying infrastructure are outside the scope of this report and are covered in the applicable UKG Dimensions SOC reports and UKG Ready and UKG Ready Partner Network SOC reports.

- **MasterTax**: MasterTax is a software solution provided by Automatic Data Processing, Inc. (ADP), a subservice organization. The Tax team is the primary user base and administers logical access to the UKGPS instance of the application. MasterTax is used by UKGPS to automate the payroll tax filing process through an import of tax liability data from the Payroll Systems into the application and by using a predefined communication format that applies to many federal, state,

and local tax jurisdictions in the United States. UKGPS leverages MasterTax to help reduce payroll tax processing time and confirm tax agency compliance for Customers. UKGPS utilizes a web-based version of the MasterTax application whereby the application and supporting infrastructure are hosted and managed by ADP. As such, controls around the maintenance, hosting, and development of the MasterTax application and supporting infrastructure are not in-scope to this report and are covered in the ADP MasterTax SOC report.

- **Bank Reconciliation Software**: UKGPS utilizes a third-party hosted reconciliation software, called Assure, to perform bank balance reconciliations for payroll-related banking transactions. The Treasury team is the primary user base and administers UKG logical access to the UKGPS instance of the application. Assure allows UKGPS the ability to analyze and validate the settlement of transactions initiated on behalf of Customers, helping to ensure prompt and proper settlement of funds. The application and supporting infrastructure are hosted and managed by a third party. As such, controls are around the maintenance, hosting, and development of the Assure application and supporting infrastructure are not in scope to this report.

- **Banking Applications**: UKGPS utilizes multiple third-party web-based applications to submit ACH and wire transactions to the financial institutions. Transactions processed by these banking applications allow UKGPS to collect Customer funds, make payroll payments on behalf of Customers, and reconcile balances. The Treasury team is the primary user base and administers logical access to the UKGPS instances of the applications.

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 the third-party hosted applications MasterTax and Assure, and the file share servers (managed by the Payroll Services Operations team). Data in transit is encrypted over secure.

The UKGPS Active Directory network housed in the Private Cloud contains key file shares used to retain internal business documents and Customer data files. These files are required to perform relevant payroll distribution and tax processing services, including those necessary to perform and evidence the key controls describe within this report.

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, 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's 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.
- Inventorying data in a way to achieve accurate reporting of processing activities conducted on behalf of Customers.

Subservice organizations complementary controls

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

- **Cyxtera Technologies, Inc. (Cyxtera):** Cyxtera 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	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 and confidentiality failures, incidents, and concerns, and other complaints.
Cyxtera Mandiant	CC2.2, CC7.3	Controls to notify UKG of any incidents or breaches.
Cyxtera	CC6.4	Controls to address physical access and environmental protections to computer equipment and storage media are established.
Cyxtera	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 communicating any identified security and confidentiality violations or incidents to UKG in a timely manner as necessary.
- User entities are responsible for controlling access to computers and devices used to communicate with UKG.
- User entities are responsible for providing UKG timely written notification of changes in individuals authorized to instruct UKG regarding activities on their behalf.
- User entities are responsible for communicating any changes in delivery destinations to UKG in a timely manner as necessary.