SOC 3 ® Report

Description of UKG Incorporated’s UKG Dimensions HCM System relevant to Security, Availability, Processing Integrity, 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 UKG INCORPORATED'S UKG DIMENSIONS HCM SYSTEM BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY, AVAILABILITY, PROCESSING INTEGRITY, CONFIDENTIALITY, AND PRIVACY 3

REPORT OF INDEPENDENT ACCOUNTANTS 4

SYSTEM DESCRIPTION OF THE UKG DIMENSIONS HCM SYSTEM.. 6

SCOPE OF THE REPORT AND OVERVIEW OF THE SERVICES 6

Product overview and service... 6
Components of the system... 7
Service commitments and requirements... 9

SUBSERVICE ORGANIZATIONS COMPLEMENTARY CONTROLS... 9

Carved-out unaffiliated subservice organizations.. 9

USER ENTITY RESPONSIBILITIES 11

Management’s Report of its Assertions on the Effectiveness of its Controls over UKG Incorporated’s UKG Dimensions HCM System Based on the Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

December 22, 2022

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

- Identifying the UKG Dimensions HCM System (System) and describing the boundaries of the System, which are presented in the section below titled *System Description of the UKG Dimensions HCM 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 Dimensions HCM System*
- Identifying, designing, implementing, operating, and monitoring effective controls over the *UKG Dimensions HCM 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 Google Cloud Platform, an external subservice organization, to provide various services, including hosting and cloud computing. Additionally, UKG uses Twilio, an external subservice organization, to provide SMS open-shift scheduling and Mandiant, an external subservice organization, to provide endpoint detection and response 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, processing integrity, 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

EY
Building a better working world

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 the UKG Dimensions HCM System* (Assertion), that UKG Incorporated's (UKG) controls over the UKG Dimensions HCM System (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, processing integrity, 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 Dimensions HCM 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 Google Cloud Platform, an external subservice organization, to provide various services, including hosting and cloud computing. Additionally, UKG uses Twilio, an external subservice organization, to provide SMS open-shift scheduling and Mandiant, an external subservice organization, to provide endpoint detection and response 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. 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, processing integrity, 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 current and prospective customers of the UKG Dimensions HCM 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
Boca Raton, Florida

System Description of the UKG Dimensions HCM 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 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 infrastructure and application services supporting the production instances of UKG Dimensions HCM System for Customers in the United States (US), Canada (CA), Australia (AU), and Europe (EU).

The scope of the Description does not include the provisioning of Customer access to the Customer's instance of the application or any Customer self-customizations (e.g., input, processing, or output field configurations) within their environment.

Product overview and service

The UKG Dimensions HCM System is a Software as a Service (SaaS) based workforce management applications with a primary focus in delivering solutions that support employee timekeeping, scheduling, leave and attendance, human resources (HR), and payroll. UKG has made various services available through different modules within the Custom Function Cloud (CFC). The CFC is an environment designed to host additional modules that can be tailored for a Customer's specific business needs. These solutions are available to Customers as add-on modules to their existing UKG Dimensions HCM System. The CFC modules communicate with UKG Dimensions via Application Programming Interfaces (APIs). The list of available CFC modules is included in the “Components of the system” section of this report. Unless otherwise noted, the UKG Dimensions HCM System and CFC solution are referred to collectively as UKG Dimensions.

UKG delivers the platform for applications and third-party offerings to be accessed within one interface. UKG Dimensions is hosted on the Google Cloud Platform (GCP) providing Customers with the benefit of high availability within the public cloud. UKG Dimensions is highly available, from anywhere through a secure, front-end interface. Customers of UKG Dimensions receive access to their solution without having to purchase additional hardware, operating systems, or database licenses.

Components of the system

Infrastructure

The infrastructure supporting the UKG product environment exists in GCP, which uses 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. The UKG product resides in multiple zones. Data is shared among the data centers within a region to provide redundancy and high availability within the region. Customer data is hosted within the UKG product environment located in GCP, in any of the regions depicted in the scope depending on the location of the Customer. This ecosystem is bordered by redundant L3 and L7 firewall technologies, which are responsible for traffic policing and policy enforcement for inbound, outbound, and internal communications. UKG users accessing the infrastructure (e.g., servers, databases) are authenticated and authorized through directory services via a Privileged Identity Management (PIM) and/or Secure Sockets Layer (SSL) Virtual Private Network (VPN) tool with multi-factor authentication (MFA). Customer specific configurations and data are segmented logically within the database. Further, a small subset of administrative UKG users has direct access to the GCP portal.

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 Dimensions application is designed, deployed, and maintained by UKG resources to be delivered to Customers using the public internet. The UKG Dimensions application is a workforce management suite that includes functionality for employee timekeeping, scheduling, leave and attendance, HR, and payroll. Boomi is a tool utilized for the integration between the UKG Dimensions application and Customer third-party systems. The Boomi tool manages key APIs within the UKG Dimensions ecosystem, as well as the APIs within external Customer environments. The UKG Dimensions application comes with Boomi accounts that allow Customers to create, deploy, and manage APIs to help enable UKG Dimensions to work seamlessly with other third-party applications. Below is a table of the modules that comprise the UKG Dimensions application and their availability by region.

Module	United States	Australia	Canada	Europe
Timekeeping[1]	X	X	X	X
Scheduling[1]	X	X	X	X
Leave & Attendance[1]	X	X	X	X
Forecasting[1]	X	X	X	X
Work[1]	X	X	X	X
Healthcare Analytics[1]	X	X	X	X
HR[2]	X	X		X
Payroll[2]	X			
Microsoft Outlook Add-on[3]	X	X	X	
SMS Open ShiftFill[3]	X	X		
Gaming[3]	X			
Rotation Schedule[3]			X	
DataHub[3]	X (Beginning on 1/13/2022)	X (Beginning on 1/12/2022)	X (Beginning on 1/13/2022)	X (Beginning on 1/13/2022)
Auctions[3]	X (Beginning on 7/21/2022)	X (Beginning on 7/27/2022)	X (Beginning on 7/14/2022)	X (Beginning on 7/14/2022)

[1] Module available via core Dimensions; [2] Module available via HCM; [3] Module available via CFC

Once a new contract is signed between UKG and a Customer, Cloud Operations creates two new core UKG Dimensions tenants (one production and one non-production tenant), as well as one Human Capital Management (HCM) tenant for HR and payroll functionality, if applicable. The non-production tenant comes equipped with baseline configurations designed for the Customer's industry. The Customer can then log into their tenant and customize the configurations to meet their business requirements.

UKG only makes changes to a Customer's environment upon Customer's request, in the event the Customer is unable to complete the task themselves. As the application is highly customizable, the 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 UKG change management controls to facilitate complete and accurate calculations of data. Implementations and changes are documented, tracked, and approved using a ticketing system.

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, 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:

- 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 UKG policy and customer commitments as applicable.
- 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'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, as applicable, and contractual requirements, as UKG products and processes evolve, utilizing the Data Inventory and Classification methodology.
- 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 UKG Dimensions system:

- **Google Cloud:** Google Cloud is utilized for computing and hosting services to store and maintain UKG Dimensions customer data.
- **Twilio:** Twilio provides SMS services for open-shift scheduling through the use of the SMS Open ShiftFill application.
- **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
Google Cloud Twilio	CC1.1, CC6.1, P4.2, P6.4, P6.7	Controls to address the monitoring and protection of customer data.
Google Cloud Twilio	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.
Google Cloud 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.
Google Cloud Twilio Mandiant	CC2.2, CC7.3, P6.3, P6.4, P6.5, P6.6	Controls to notify UKG of any incidents or breaches.
Google Cloud Twilio	CC6.1, CC6.2, CC6.3	Controls to address logical access to application software, system software, databases, and network components is restricted to authorized and appropriate users to perform authorized and appropriate actions.
Google Cloud	CC6.1, A1.2	Controls to encrypt data at rest in the Google Cloud.
Google Cloud	CC6.4	Controls to address physical access and environmental protections to computer equipment and storage media are established.
Google Cloud Twilio	CC6.6, CC7.2 C1.2, P6.3 P6.4	Controls to address that the entity’s network is monitored and security mechanisms exist to protect from external threats and interruptions.
Google Cloud	CC6.7	Controls to prevent equipment from leaving Google data centers without being subject to Google’s sanitization process.
Google Cloud Twilio	CC8.1	Controls to address the handling and protection of confidential data during the system development lifecycle.
Google Cloud Twilio	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 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 reviewing notifications from UKG of changes to the System and communicating any concerns to UKG.
- 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.
- User entities are responsible for the security and management of their network and infrastructure, including implementing appropriate protections against malicious software and unauthorized access.
- 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.
- User entities are responsible for managing UKG access to their tenants.
- User entities are responsible for appropriately securing transmissions of data to UKG (including transmission strength) and informing UKG of any necessary changes to the System.
- User entities are responsible for communicating any identified incidents impacting the security, availability, confidentiality, or processing integrity of the system to UKG on a timely basis.
- User entities are responsible for reviewing changes to their data to ensure that changes are appropriate and authorized.
- User entities are responsible for approving the list of users authorized to approve configuration items prior to go-live.
- 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 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 monitoring the completion status of APIs and investigating any integration failures.
- User entities are responsible for ensuring that changes to APIs post go live, including any configurations, are authorized, tested, and approved.
- User entities are responsible for the completeness and accuracy of data input to the System via either direct data input or API.
- User entities are responsible for reviewing all configurations and APIs that are part of their UKG Dimensions environment prior to providing the UAT signoff in the implementation process.
- User entities are responsible for determining that the transaction processing functionality within the UKG Dimensions application meets their expectations and notifying UKG timely with any required changes or enhancements.
- User entities are responsible for reviewing system outputs for completeness and accuracy and notifying UKG of any discrepancies.
- User entities are responsible for monitoring all required scheduled jobs for timeliness and completeness and notifying UKG if support is required.

- 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 facilitating data subject requests by submitting support cases to UKG.
- User entities are responsible for providing physical and electronic copies of personal information upon the data subject's request. Denial to provide such information is communicated to the data subject by the entity.